



BITDEFENDER SECURITY FOR FILE SERVERS

Administratorhandbuch

BitDefender Security for File Servers 3.5 *Administratorhandbuch*

Veröffentlicht 2011.04.18

Copyright© 2011 BitDefender

Rechtlicher Hinweis

Alle Rechte vorbehalten. Bestandteile dieses Handbuches dürfen weder in elektronischer noch mechanischer Form reproduziert werden. Dies gilt auch für das Fotokopieren, Aufnehmen oder jegliche andere Form von Datenspeicherung oder Informationsbeschaffung, ohne die Zustimmung von BitDefender. Ausnahmen gelten für Zitate in Verbindung mit Testberichten. Der Inhalt darf in keiner Weise verändert werden.

Warnung und Haftungsausschluss. Dieses Produkt bzw. Dokument ist urheberrechtlich geschützt. Die inhaltlichen Informationen in diesem Dokument sind „faktenbasiert“ und enthalten keinen Garantieanspruch. Obwohl dieses Dokument mit äußerster Sorgfalt erstellt und geprüft wurde, übernehmen die Autoren keinerlei Haftung für eventuell auftretende Schäden bzw. Datenverlust die direkt oder indirekt unter Verwendung dieses Dokumentes entstehen könnten oder bereits entstanden sind.

Dieses Handbuch enthält Verweise auf andere, nicht von BitDefender erstellte Webseiten, die auch nicht von BitDefender kontrolliert werden. Somit übernimmt BitDefender auch keine Verantwortung für den Inhalt dieser Webseiten. Der Besuch dieser Webseiten erfolgt somit auf eigene Gefahr. BitDefender stellt diese Verweise aus Gründen der Anwenderfreundlichkeit zur Verfügung, was nicht bedeutet, dass BitDefender in jeglicher Art und Weise Verantwortung oder Haftung für diese Webseiten und deren Inhalt übernimmt.

Warenzeichen. Es erscheinen eingetragene Warenzeichen in diesem Dokument. Alle eingetragenen und nicht eingetragenen Warenzeichen in diesem Dokument sind das alleinige Eigentum der jeweiligen Besitzer.



Inhaltsverzeichnis

- Vorwort vii**
 - 1. Verwendete Konventionen vii
 - 1.1. Typografie vii
 - 1.2. Symbole viii
 - 2. Struktur viii
 - 3. Ihre Mithilfe ix
- Beschreibung 1**
 - 1. Funktionen und Vorteile 2**
 - 1.1. Hauptmerkmale 2
 - 1.2. Hauptvorteile 2
 - 1.3. Dienste 3
 - 1.4. Erweiterte BitDefender Technologien: 3
 - 2. Funktionsdiagramm für Endnutzer 4**
- Installation 6**
 - 3. Vor der Installation 7**
 - 3.1. Systemanforderungen 7
 - 4. BitDefender Security for File Server installieren 8**
 - 4.1. Neue Installation 8
 - 4.1.1. Schritt 1/8 - Willkommen 9
 - 4.1.2. Schritt 2/8 - Endbenutzer-Lizenzvereinbarung 9
 - 4.1.3. Schritt 3/8 - Prüfung vor der Installation 10
 - 4.1.4. Schritt 4/8 - Zu installierende Produkte auswählen 11
 - 4.1.5. Schritt 5/8 - Produkt-Update-Optionen konfigurieren 12
 - 4.1.6. Schritt 6/8 - Vorfallsberichte 13
 - 4.1.7. Schritt 7/8 - Installation starten 14
 - 4.1.8. Schritt 8/8 - Installation abgeschlossen 14
 - 4.2. Bestehende Installation ändern 15
 - 4.3. Upgrade für eine ältere Version installieren 15
 - 5. BitDefender ändern, reparieren oder entfernen 16**
 - 5.1. Modifiziere BitDefender 16
 - 5.2. BitDefender reparieren 17
 - 5.3. BitDefender deinstallieren 17
- Konfiguration und Verwaltung 18**
 - 6. Erste Schritte 19**
 - 6.1. BitDefender Symbol im Infobereich der Taskleiste 20
 - 6.2. Verbindung zu einem anderen Computer herstellen 21
 - 6.3. Administratives Passwort ändern 22
 - 6.4. importieren/exportieren der Management Konsole Einstellungen 23
 - 6.4.1. Policy-Einstellungen exportieren 23
 - 6.4.2. Policy-Einstellungen importieren 23
 - 7. Registrierung und Mein Benutzerkonto 26**

7.1. Schritt 1/3 - BitDefender Security for File Server registrieren	27
7.2. Schritt 2/3 - BitDefender Benutzerkonto registrieren	28
7.3. Schritt 3/3 - Fertigstellen	30
8. Überwachung	31
8.1. Dashboard	32
8.1.1. Wichtige Links	33
8.1.2. Statusbereich	33
8.1.3. Prüfkaktivität	38
8.1.4. Produkt-Status	39
8.2. Statistik	39
8.2.1. Statistiken säubern	40
8.3. Berichte	41
8.3.1. Berichte verwalten	42
8.3.2. Berichte erstellen	43
8.4. Benachrichtigungen & Protokolle	47
8.4.1. Benachrichtigungen	47
8.4.2. Protokolle	58
8.5. Quarantäne	60
8.5.1. Die Quarantäne verwalten	61
8.6. Geplante Aufgaben	62
8.6.1. Geplante Aufgaben verwalten	63
8.6.2. On-Demand Prüfaufgaben	64
8.6.3. Update-Aufgaben	83
8.6.4. Aufgaben zur Berichterstellung	89
9. Serverprüfung	99
9.1. Echtzeitschutz	100
9.1.1. Sicherheitsstufe einstellen	101
9.1.2. Sicherheitsstufe einstellen	102
9.1.3. Anzahl der Prüfinstanzen konfigurieren	110
9.2. Prüfvorgang	111
9.2.1. Dateien und Ordner prüfen	113
9.2.2. Konfiguration der On-Demand-Prüfeinstellungen	119
9.3. Prüfausnahmen	129
9.3.1. Globale Ausnahmen	129
9.3.2. Prozessausnahmen	131
9.3.3. Manuell auszuschließende Elemente	132
9.4. AntiViren-Schutz Prüfung	133
10. Aktualisierung	135
10.1. Aktualisierung	136
10.1.1. Update-Informationen	136
10.1.2. Produkt-Update	136
10.2. Update-Einstellungen	138
10.2.1. Update-Planung konfigurieren	138
10.2.2. Konfiguriere Produkt Updates	139
10.3. Update Locations	141
10.4. Update Benachrichtigungen	142
10.5. Update zurückrollen	144
11. Allgemein	145
11.1. Virenbericht	145
11.2. Vorfallsberichte	146

11.3. Tray Icon 147

Fehlerdiagnose und Problemlösung 149

12. BitDefender Konfigurationsreparatur Tool 150

13. Support 152

13.1. BitDefender-Support-Center 152

13.1.1. BitDefender Knowledge Base 152

13.1.2. BitDefender Support-Forum 153

13.1.3. Video Tutorials 153

13.1.4. Produktdokumentation 153

13.2. Hilfe anfordern 153

13.3. BitDefender Support Tool 154

14. Kontaktinformation 157

14.1. Kontaktadressen 157

14.2. Händler vor Ort 157

14.3. BitDefender Geschäftsstellen 157

14.3.1. Deutschland 158

14.3.2. USA 158

14.3.3. Großbritannien und Irland 158

14.3.4. Spain 158

14.3.5. Rumänien 159

Glossar 160

Vorwort

Dieses Benutzerhandbuch ist für alle Unternehmen vorgesehen, die sich für **BitDefender for File Server** als Sicherheitslösung für ihre File Server entschieden haben. Die in diesem Dokument beschriebenen Informationen sind nicht nur für IT-Profis gedacht, sondern auch für all diejenigen die unter Windows arbeiten können.

Dieses Handbuch beschreibt **BitDefender for File Server** die Firma und das Team die es konzipiert haben, es wird Sie durch den Installationsprozess führen und Ihnen zeigen wie Sie das Produkt konfigurieren können. So lernen Sie wie Sie **BitDefender Security for File Server** verwenden, aktualisieren, testen und anpassen können. So erfahren Sie wie Sie BitDefender am Effektivsten einsetzen können.

Viel Spaß mit diesen nützlichen und informativen Handbuch.

1. Verwendete Konventionen

1.1. Typografie

Um die Lesbarkeit zu fördern werden verschiedene Arten von Textstilen verwendet. Die jeweiligen Bedeutungen entnehmen Sie bitte der Tabelle unterhalb.

Erscheinungsbild	Beschreibung
<code>sample syntax</code>	Syntaxbeispiele werden in einer Schriftart mit <i>fester Laufweite</i> angegeben.
http://www.bitdefender.com	Verweise (Links) auf externe Inhalte wie z.B. Web-Seiten oder FTP-Server.
sales@bitdefender.com	Verweise auf E-Mail-Adressen, z.B. zur Kontaktaufnahme.
„Vorwort“ (S. vii)	Interne Verweise (Links) auf beliebige Stellen innerhalb dieses Dokuments.
<code>filename</code>	Dateien und Verzeichnisse werden in einer Schriftart mit <i>fester Laufweite</i> angegeben.
option	Optionen wie z.B. Schaltflächen oder Checkbox-Elemente werden in fett gedruckt angegeben.
<code>sample code listing</code>	Beispielquelltexte werden in einer Schriftart mit <i>fester Laufweite</i> angegeben.

1.2. Symbole

Bei diesen Symbolen handelt es sich um Hinweise innerhalb des Textflusses welche mit einer kleinen Grafik markiert sind. Hierbei handelt es sich um Informationen die Sie in jedem Fall beachten sollten.



Beachten Sie

Diese Bemerkung dient lediglich zur Überprüfung. Notizen enthalten nützliche Informationen wie zum Beispiel einen Verweis auf ein verwandtes Thema.



Wichtig

Diese Art von Hinweis sollte in jedem Fall gelesen werden. Es werden signifikante Informationen zum jeweiligen Thema bereitgestellt. Es wird nicht empfohlen diese zu übergehen.



Warnung

Diese kritische Information sollten Sie mit höchster Aufmerksamkeit verfolgen. Hier angegebenen Anweisungen und Informationen sollten Sie auf jeden Fall Beachtung schenken. Sie sollten diese Informationen sorgsam lesen und verstanden haben, da es sich um eine höchst prekäre Thematik handelt.

2. Struktur

Dieses Handbuch ist in vier Abschnitte unterteilt, welche die folgenden Hauptthemen beinhalten: Beschreibung, Installation, Konfiguration und Verwaltung, Fehlerdiagnose und Problemlösung. Ausserdem ist ein Glossar enthalten welcher einige technische Begriffe erklärt.

Beschreibung. BitDefender Security for File Server und dessen Funktionen werden vorgestellt.

Installation. Schritt-für-Schritt Anleitung zur Installation von BitDefender an einem Arbeitsplatz. Hierbei erhalten Sie ausführliche Informationen für eine erfolgreiche Installation von **BitDefender for File Server**. Beginnend mit den Installationsvoraussetzungen werden Sie durch den gesamten Installationsprozess begleitet. Zusätzlich wird beschrieben wie eine Deinstallation von BitDefender durchzuführen ist.

Konfiguration und Verwaltung. Beschreibung der Grundkonfiguration und Wartung von BitDefender. Diese Abschnitte erklären alle Optionen von **BitDefender Security for File Server**, wie das Produkt zu registrieren ist, wie ein Prüfvorgang für den File Server und wie ein Update von BitDefender durchgeführt werden kann.

Fehlerdiagnose und Problemlösung. Beschreibt wie Sie Hilfe bzw. Unterstützung zu dem Produkt erhalten und erhält zusätzlich eine Liste mit den am häufigsten gestellten Fragen (FAQ).

Glossar. Im Glossar werden technische Ausdrücke und seltene Bezeichnungen erklärt, die in diesem Dokument zu finden sind.

3. Ihre Mithilfe

Wir laden Sie dazu ein uns bei der Verbesserung dieses Dokuments mitzuhelfen. Wir haben sämtliche Informationen in diesem Dokument bestmöglich überprüft um somit die Qualität sicherzustellen.

Falls Sie dennoch Fehler finden, so teilen Sie uns diese bitte mit indem Sie uns per E-Mail unter der Adresse documentation@bitdefender.com kontaktieren.



Wichtig

Bitte verfassen Sie bitte alle auf die Dokumentation bezogenen E-Mails auf Englisch.

Beschreibung

1. Funktionen und Vorteile

BitDefender Security for File Server bietet einen effizienten Schutz für die Speicherpunkte ihres Unternehmens.

BitDefender Security for File Servers ist eine Lösung, die speziell auf Windows basierte Server zugeschnitten und einfach zu installieren ist. Der Datenverkehr wird gegen Viren, Spyware und Rootkits geschützt, wobei der Verwaltungsaufwand für eine Server-Software Lösung minimiert wird.

1.1. Hauptmerkmale

- Verbesserter Schutz (Antivirus, Antispyware, Antirootkit) für den Datenverkehr.
- Proaktiver und heuristischer Schutz vor Zero-Day Threats
- Optimierte Prüfung für schnelleren Dateizugriff
- Multithread-Prüfung verkürzt merklich die benötigte Prüfzeit
- On-Access (bei Zugriff) und On-Demand (auf Anfrage) Scanner bieten umfangreichen File Server Schutz
- Die Kompatibilität mit der zentralen Verwaltungskonsole erleichtert die administrative Arbeit
- 64 bit Support

1.2. Hauptvorteile

- Erhöhte Leistungsfähigkeit
 - ☐ Prüft "schreibgeschützte" Dateien nur einmal im Verlauf einer Sitzung und prüft sie erst wieder, wenn eine neue Sitzung eröffnet wird, wenn ein Update ansteht oder eine Infizierung des Systems festgestellt wird.
 - ☐ Dank seiner fortgeschrittenen Multithread Prüffunktion, wird ein sekundenschneller und sicherer Dateizugriff gewährleistet.
 - ☐ Bietet Funktionen für die zeitliche Steuerung für On-Demand-Scans und Updates.
 - ☐ Mit dem Alarmmodul werden Sie über den Prüfungsvorgang und Updates informiert
- Sichere gemeinsame Benutzung von Dateien und Dokumenten
 - ☐ Kopierte Dateien oder Dateien, auf die zugegriffen wurde, werden in Echtzeit geprüft, ohne dass dies Einfluss auf die Serverleistung hat.
 - ☐ Erlaubt die zeitliche Planung von On-Demand Virenskans oder die Ausführung einer sofortigen Prüfung, zur Verbesserung der Sicherheit des File-Servers.
- Verbesserte Benutzerfreundlichkeit
 - ☐ Bietet verbesserte Verwaltungsfunktionen und erlaubt einen schnellen Zugang zu den wichtigsten Einstellungen, dank seiner benutzerfreundlichen und intuitiven MMC-basierenden Benutzeroberfläche.
 - ☐ Zeigt Informationen über kritische Ereignisse an und über das neue Dashboard kann über eine Taste direkt darauf zugegriffen werden.

- ☐ Mithilfe des verbesserten Überwachungssystems und einem speziellen Statistik-Modul werden Berichte über die Produktaktivität geliefert.
- ☐ Es können benutzerdefinierte Benachrichtigungen für verschiedene Ereignisse gesendet werden, wie: Antivirus Signatur-Updates, Produkt Updates, On-Demand Prüfungen oder entdeckte Viren.
- Zentrale Verwaltung

Mit dem BitDefender Management Server können die meisten BitDefender Business Lösungen, die auf den Netzwerkcomputern installiert sind, zentral verwaltet werden, einschließlich der Lösung BitDefender Security for File Server. Durch diese Integration können Sie die Management Server Konsole für einen zentralen Zugriff auf folgende Optionen verwenden:

- ☐ Konfiguration der Einstellungen von BitDefender Security for File Server
- ☐ Informationen über wichtige Ereignisse, so wie Updates, Konfigurationswarnungen, Lizenzablauf
- ☐ Leicht verständliche Statistiken und Berichte, die auf den Informationen basieren, die von BitDefender Security for File Server erhalten wurden

1.3. Dienste

- Fortgeschrittenes Update-System
Für einen dauerhaften Schutz, erhält die Lösung ständig die neusten Updates und Patches, wobei Sie den Zeitpunkt der Aktualisierung wählen können: On-Demand, zeitlich konfiguriert oder automatisch.
- Upgrades
Registrierte Nutzer profitieren von kostenfreien Upgrades auf jede neue Version des für sie lizenzierten Produktes während der gesamten Lizenzlaufzeit. Für ehemalige Kunden stehen ebenfalls spezielle Angebote zur Verfügung.
- Kostenloser Technischer 24-Stunden Support
Geprüfte Mitarbeiter stehen BitDefender Business Kunden mit einem kostenlosen 24-Stunden Support zur Verfügung, sowohl Online, als auch per Telefon oder E-Mail. Zusätzlich steht eine Online-Datenbank zur Verfügung, mit Antworten zu häufig gestellten Fragen, und oft behandelten Themen.

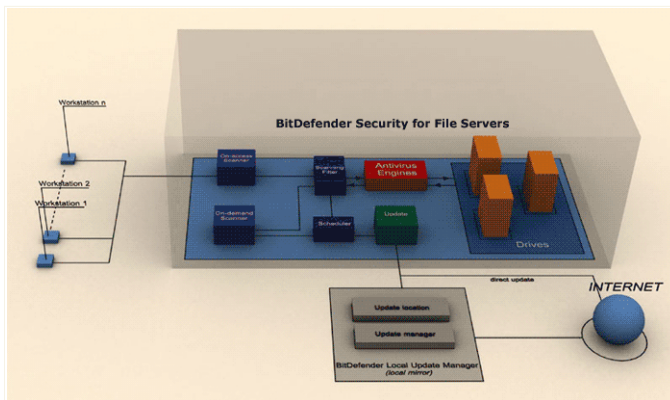
1.4. Erweiterte BitDefender Technologien:

B-HAVE. BitDefender Security for File Server beinhaltet B-HAVE, eine patentierte Technologie, die das Verhalten potentiell gefährlicher Codes innerhalb einer virtuellen Umgebung analysiert, wobei False Positives beseitigt werden und die Erkennungsrate für neue und unbekannte Malware erheblich gesteigert wird.

Zertifizierte Antivirus Engines. Die Scan Engines von BitDefender wurden mit ihrer B-HAVE Technologie bereits mehrfach von ICSSA Labs, Virus Bulletin und Checkmark für den besten vorbeugenden Virenschutz, der zurzeit erhältlich ist, ausgezeichnet.

2. Funktionsdiagramm für Endnutzer

Das unten abgebildete Funktionsdiagramm zeigt, wie BitDefender arbeitet.



Funktionsdiagramm

Um als Sicherheitslösung für Server optimal arbeiten zu können basiert **BitDefender Security for File Server** auf einer modularen Architektur. Dies sind die wichtigsten Module:

- **On-access Scanner**
- **On-demand Scanner**
- **Update**
- **Aufgabenplaner**
- **Antivirus Engines**

Echtzeitschutz. Wenn Dateien auf die Festplatte geschrieben werden oder auf sie zugegriffen wird, erkennt das Modul On-Access Scanner das Ereignis und startet eine Prüfung.

Der Prüfprozess beinhaltet die folgenden Schritte:

1. Nacheinander werden Dateiendung, Dateigröße und Pfad auf Übereinstimmung mit den Administrator-Konfigurationen hin überprüft. Das Ergebnis des Filtervorgangs ist entweder SCAN oder NICHT PRÜFEN.
2. Wenn das Ergebnis SCAN ist, wird die Datei von den Antivirus-Engines geprüft. Zunächst wird die Datei mit der Antivirus-Signaturdatenbank abgeglichen. Wenn irgendein Teil der Datei mit einer Signatur übereinstimmt, wird die Datei als infiziert gemeldet. Wenn keine Übereinstimmung gefunden wird, wird die Datei mit der B-HAVE-Technologie geprüft. Falls die Datei ein Verhalten zeigt, dass Malware-Charakteristika hat, wird die Datei als infiziert gemeldet. Das Ergebnis des Antivirusmoduls kann INFIZIERT oder SAUBER sein.

3. Wenn die Datei nach der Prüfung durch das Antivirus-Modul INFIZIERT ist, kann eine der folgenden Aktionen ausgeführt werden: desinfizieren, löschen, in die Quarantäne verschieben. Wenn diese Aktionen fehlschlagen, wird die Aktion **Zugriff verweigern** ausgeführt, sodass der Benutzer den Schad-Code nicht ausführen kann.

On-Demand-Prüfung. Der On-Demand Scanner kann von der Benutzeroberfläche aus über **Jetzt prüfen** oder über eine voreingestellte On-Demand-Prüfaufgabe durchgeführt werden. Der Prüfprozess entspricht dem Prüfvorgang in Echtzeit. Der Unterschied besteht darin, dass die On-Demand-Prüfung nicht für die Dateien angewendet wird, auf die zugegriffen wurde sondern auf solche, die von dem Benutzer aus diesem Grund ausgewählt wurden.

Update. Das Update-Modul führt den Update-Prozess durch und die Hauptfunktion besteht darin, die aktuellsten Dateien von BitDefender herunterzuladen. Drei Dateitypen stehen zur Verfügung:

- **Antivirus-Signaturen** - Diese Dateien werden ständig aktualisiert, da das BitDefender Labor täglich neue Viren aktualisiert.
- **Antivirus Engines** - Diese Dateien werden so häufig aktualisiert wie die Antivirus-Signaturen B-HAVE, eine patentierte BitDefender-Technologie, in die Antivirus Engines implementiert wurden.
- **Produktdateien** - Die Aktualisierung der Produktdateien unterscheidet sich vom Update der Antivirus-Signaturen und Ihre Funktion besteht darin, Problemlösungen und Leistungsverbesserungen des Produktes zu liefern. Produkt-Updates werden heruntergeladen, jedoch nicht automatisch installiert. Bitte beachten Sie dass die Installation von Produkt-Updates einen Systemneustart erfordern kann.



Beachten Sie

Der Update-Prozess wird automatisch jede Stunde durchgeführt, jedoch kann das Zeitintervall geändert und die Update-Aufgaben zu jedem gewünschten Zeitpunkt eingestellt werden.

Installation

3. Vor der Installation

Zur Vorbereitung der Installation müssen Sie die folgenden Schritte ausführen:

- Stellen Sie sicher, dass der Computer die **Systemanforderungen** erfüllt.
- Melden Sie sich als Administrator am Computer an.
- Entfernen Sie ähnliche Sicherheits-Software vom Computer. Die gleichzeitige Nutzung mehreren Sicherheitsprogrammen kann die jeweilige Funktion stören und massive Probleme auf Ihrem Computer verursachen.

3.1. Systemanforderungen

Software-Anforderungen

- **Betriebssystem:**
 - ☐ Windows 2000 SP4 und Update Rollup 1 Version 2
 - ☐ Windows Server 2003 SP1
 - ☐ Microsoft Windows Server 2008 / Microsoft Windows Server 2008 R2
- Internet Explorer 6

Hardware-Anforderungen

64-bit:

- Alle Windows-Prozessoren (Intel oder AMD)
- Minimum 1 GB freier Speicherplatz auf der HDD

32-bit:

- Minimum Prozessor - Pentium III 500 MHz
- 256 MB Arbeitsspeicher - 512 MB empfohlen
- Minimum 1 GB freier Speicherplatz auf der HDD

4. BitDefender Security for File Server installieren

Um BitDefender Security for File Servers zu installieren, benötigen Sie eine Installationsdatei oder eine CD, die das Installationspaket beinhaltet. Abhängig von dem jeweiligen Business Produkt, hat die Datei einen anderen Namen. Sie können die Installationsdatei von www.bitdefender.de herunterladen.

Es gibt zwei Versionen des Installationspakets:

- **32-bit** - Benutzen Sie diese Version, zur Installation von BitDefender Security for File Server auf einem 32-bit Computer.
- **64-bit** - Benutzen Sie diese Version, zur Installation von BitDefender Security for File Servers auf einem 64-bit Computer.

Das Installationspaket beinhaltet, ausser BitDefender Security for Windows Server, auch noch andere BitDefender Security for File Servers Produkte. Sie sollten alle Produkte, die Sie benutzen wollen, zur gleichen Zeit installieren. Installieren Sie nur BitDefender Security for File Servers, werden Sie bei der späteren Installation anderer BitDefender Produkte, die existierende Installation modifizieren müssen. Als resultat dieser Aktion, kann es nötig sein einige Dateien zu ersetzen. Dies kann dazu führen, dass temporär einige installierte Produkte nicht richtig funktionieren.

Je nachdem, ob Sie bereits Produkte aus dem Paket auf Ihrem Computer installiert haben, gibt es zwei Wege BitDefender Security for File Servers zu installieren:

- **Neue Installation** - kein anderes Produkt des Installationspakets ist auf dem Computer installiert.
- **Bestehende Installation ändern** - mindestens ein anderes Produkt des Installationspaketes ist auf dem Computer installiert.

4.1. Neue Installation

Um eine Neue Installation zu starten, doppelklicken Sie auf die Installationsdatei. Ein Assistent wird eingeblendet; folgen Sie seinen Anweisungen, um die Installation fertigzustellen.

Bevor die Installation beginnt, prüft BitDefender, ob eine neuere Version des Installationspaketes verfügbar ist. Sollte dies der Fall sein, so werden Sie gefragt, ob Sie dieses herunterladen möchten. Klicken Sie **Ja** um die neue Version herunterzuladen oder **Nein** um die Installation mit der bereits vorhandenen Datei fortzuführen.

Befolgen Sie die folgenden Schritte um BitDefender Security for File Server zu installieren:

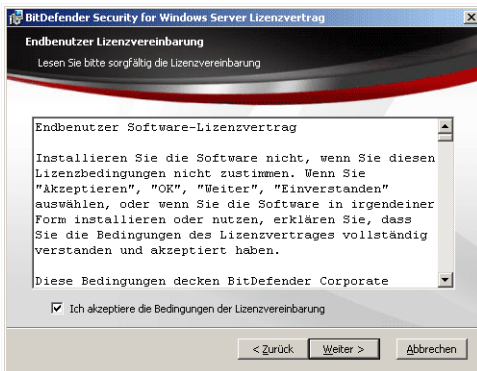
4.1.1. Schritt 1/8 - Willkommen



Willkommen

Klicken Sie auf **Weiter**, um fortzufahren, oder klicken Sie auf **Abbrechen**, um die Installation abzubrechen.

4.1.2. Schritt 2/8 - Endbenutzer-Lizenzvereinbarung



Endbenutzer-Lizenzvereinbarung

Bitte lesen Sie die Lizenzvereinbarung und wählen Sie **Ich akzeptiere die Bedingungen der Lizenzvereinbarung** und klicken Sie auf **Weiter**.



Beachten Sie

Wenn Sie diesen Bedingungen nicht zustimmen, klicken Sie auf **Abbrechen**. Die Installation wird abgebrochen und Sie werden das Setup verlassen.

4.1.3. Schritt 3/8 - Prüfung vor der Installation



Prüfung vor der Installation

BitDefender kann vor der Installation kritische Bereiche Ihres Systems prüfen, um sicherzustellen, dass der Server frei von Infektionen ist.

Die Prüfung kann einige Minuten dauern. Klicken Sie auf **Jetzt prüfen**, um die Prüfung zu starten, oder klicken Sie auf **Prüfung überspringen**, um die Installation ohne Prüfung fortzusetzen.



Wichtig

Es wird dringend empfohlen, die Prüfung durchzuführen. Aktive Malware könnte die Installation stören oder sogar dazu führen, dass die Installation fehlschlägt. Falls eine Bedrohung entdeckt werden sollte, kann ein Neustart nötig sein, um sie zu entfernen.

4.1.4. Schritt 4/8 - Zu installierende Produkte auswählen



Zu installierende Produkte auswählen

Wählen Sie BitDefender Security for File Server, klicken Sie auf den entsprechenden **Pfeil** und klicken Sie dann auf **Wird auf lokaler Festplatte installiert** in dem Shortcut-Menü.

Der Standard Installationsordner wird in der unteren Hälfte des Fensters angezeigt. Um einen anderen Ordner zu wählen, klicken Sie **Browse**, wählen Sie den Ordner und klicken Sie dann **OK**, um den Ort festzulegen.

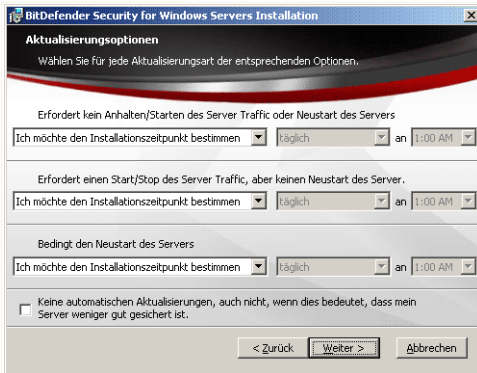


Beachten Sie

Sie können auch andere BitDefender-Produkte für Windows-Server installieren. Wählen Sie sie wie oben beschrieben aus. Je nach gewähltem Produkt können einige zusätzliche Schritte im hier beschriebenen Installationsprozess auftauchen.

Klicken Sie auf **Weiter**.

4.1.5. Schritt 5/8 - Produkt-Update-Optionen konfigurieren



Produktaktualisierungsoptionen

Produkt Updates regelmäßig zu installieren, ist für die Sicherheit Ihres Servers sehr wichtig. Abhängig von dem Grad der Beeinträchtigung des Servers, gibt es drei Arten von Produkt Updates:

- Produkt Updates, die kein anhalten des Server Verkehrs oder Neustart des Servers verlangen
- Produkt Updates, die ein Anhalten des Server Verkehrs verlangen, aber keinen Neustart des Servers
- Produkt Updates, die einen Neustart des Server verlangen

Um automatische Downloads und Installation für jede Art von Produkt Updates zu konfigurieren, wählen Sie eine der folgenden Optionen:

Automatisch installieren

Wählen Sie diese Option und BitDefender wird automatisch Produkt Updates laden und installieren. Dies ist die empfohlene Wahl für Produkt Updates, die kein Anhalten des Server Verkehrs oder Neustart des Servers verlangen.

Zu einer von mir bestimmten Zeit installieren

Wählen Sie diese Option, wenn sie wollen, dass BitDefender verfügbare Updates zu einer gewissen Zeit installiert. Wählen Sie aus der Liste das Datum (Tag und Zeit) wann dies geschehen soll.

Auf diese Weise können Sie BitDefender konfigurieren Produkt Updates an Zeiten durchzuführen, zu denen die wenigsten Störungen der Server Aktivität zu erwarten sind (nachts bspw.)

Ich möchte den Installationszeitpunkt bestimmen

Wählen Sie diese Option, wenn Sie wollen, dass BitDefender automatisch Produkt Updates lädt, sie aber entscheiden, wann sie installiert werden sollen. Dies ist

die empfohlene Auswahl für Produkt Updates, die ein Anhalten des Server Verkehrs und einen Neustart des Servers verlangen.

Um die automatische Produktaktualisierung zu deaktivieren, markieren Sie das Kästchen **Keine automatischen Produktaktualisierungen, auch nicht wenn dadurch mein Server weniger gut gesichert ist.**

Klicken Sie auf **Weiter**.

4.1.6. Schritt 6/8 - Vorfallsberichte



Vorfallsberichte

BitDefender Security for File Servers enthält ein Vorfall Management Modul, welches es erlaubt während eines Produktabsturzes Berichte zu erstellen. Durch Ihre Zustimmung Vorfallsberichte an das BitDefender Labor zu senden, helfen Sie uns schnelle Problemlösungen zu finden. Sie könnten einen grossen Beitrag zur der Entwicklung eines stabilen Produktes machen, dass Ihren Wünschen entspricht. Die Berichte werden nur für statistische Zwecke genutzt, die Daten werden niemals kommerziell genutzt oder an dritte weitergegeben.

Um Vorfallsberichte an das BitDefender Labor zu senden, wählen Sie **Ich bin damit einverstanden Berichte an das BitDefender Labor zu senden** und geben Sie Ihre E-Mail-Adresse ein.

Klicken Sie auf **Weiter**.

4.1.7. Schritt 7/8 - Installation starten



Installation starten

Klicken Sie auf **Installieren**, um den Installationsvorgang zu starten.

Es dauert einige Minuten, bis die Installation abgeschlossen ist. Es werden detaillierte Informationen zum Installationsprozess angezeigt, damit Sie ihn nachvollziehen können.

4.1.8. Schritt 8/8 - Installation abgeschlossen



Installation abgeschlossen

Klicken Sie auf **Fertigstellen**, um das Fenster zu schließen. Sie werden möglicherweise aufgefordert, Ihren Computer neuzustarten, damit der Setup-Assistent die Installation beenden kann.

4.2. Bestehende Installation ändern

Um BitDefender Security for File Servers zu installieren, wenn bereits eine oder mehrere BitDefender Security for Windows Server Produkte auf Ihrem System installiert sind, müssen Sie diesen Schritten folgen.

1. Wählen Sie im Windows-Startmenü folgenden Eintrag: **Start → Programme → BitDefender Security for Windows Servers → Ändern, Reparieren oder Deinstallieren.**



Beachten Sie

Sie können auch auf die Installationsdatei von BitDefender Security for Windows Servers doppelklicken.

Wenn das Begrüßungsfenster auf geht, klicken Sie **Weiter**, um zu starten.

2. Wählen Sie **Modifizieren**.
3. Sie haben Schritt 4 des **Installationsassistenten** erreicht. Folgen Sie den Anweisungen des Assistenten, um die Installation fertigzustellen.

4.3. Upgrade für eine ältere Version installieren

Wenn Sie eine ältere Version des Produkts bereits verwenden, können Sie sie auf Version 3.5 aktualisieren, indem Sie den Installer ausführen. Folgen Sie den in „**Neue Installation**“ (S. 8) beschriebenen Anweisungen des Assistenten, um das Upgrade abzuschließen.

Wenn Sie das Upgrade von Version 3.4 auf 3.5 ausführen, werden alle Einstellungen beibehalten. Upgrades von älteren Versionen werden in der Standardkonfiguration installiert.



Beachten Sie

Das System muss neu gestartet werden, damit das Upgrade abgeschlossen werden kann.

5. BitDefender ändern, reparieren oder entfernen

Wenn Sie BitDefender ändern, reparieren oder entfernen möchten, folgen Sie dem Pfad: **Startmenü → Alle Programme → BitDefender Security for Windows Servers → Ändern, Reparieren oder Entfernen**.

Klicken Sie im Willkommensbildschirm auf **Weiter**. Ein neues Fenster wird erscheinen, in dem Sie folgendes wählen können:

- **Modifizieren** - um neue BitDefender Produkte für Windows Server zu installieren oder um kürzlich installierte Produkte zu entfernen.
- **Reparieren** - um BitDefender Security for File Servers zu re-installieren.
- **Entfernen** - dient zum Entfernen aller installierten Komponenten.



Modifiziere, Repariere oder entferne BitDefender

5.1. Modifiziere BitDefender

Das BitDefender Security for File Servers Installationspaket ist Teil eines grösseren Packets, dass alle verfügbaren BitDefender Security for Windows Servers Produkte enthält.

Wenn Sie **Modifizieren** wählen, öffnet sich ein neues Fenster, in dem Sie wählen können welche BitDefender Produkte installiert oder entfernt werden sollen.

Sie sollten alle Produkte, die Sie benutzen wollen, zur gleichen Zeit installieren.

Um ein Produkt zu installieren, klicken Sie auf den entsprechenden **Pfeil** und klicken Sie dann auf **Wird auf lokaler Festplatte installiert** in dem Shortcut-Menü.

Um ein Produkt zu deinstallieren, klicken Sie auf den entsprechenden **Pfeil** und klicken Sie dann auf **Gesamtes Merkmal wird nicht verfügbar sein** in dem Shortcut-Menü.

5.2. BitDefender reparieren

Sollte BitDefender Security for File Servers sich unerwartet verhalten, können Sie es reparieren, um die Funktionalität wieder her zu stellen. Der Reparaturprozess besteht aus einer Neu-Installation des Produktes.



Wichtig

Wir empfehlen Ihnen, vor der Instandsetzung des Produktes die Basiseinstellungen zu speichern. Nach dem Instandsetzungsvorgang können alle Einstellungen wieder geladen werden. Für weitere Informationen lesen Sie bitte *„importieren/exportieren der Management Konsole Einstellungen“ (S. 23)*

Wenn Sie **Reparieren** wählen, öffnet sich ein neues Fenster. Klicken Sie auf **Reparieren** um die Reparatur zu starten.



Wichtig

Während des Reparaturvorgangs werden alle installierten BitDefender Produkte kurzzeitig aufhören zu funktionieren.

5.3. BitDefender deinstallieren

Wenn Sie alle BitDefender Produkte deinstallieren wollen, wählen Sie **Entfernen**.



Beachten Sie

Wir empfehlen die Option **Entfernen** zu verwenden um eine saubere Neuinstallation durchzuführen.

Wenn Sie BitDefender entfernen wählen erscheint ein neues Fenster. Damit die Objekte in der Quarantäne zu bleiben, darf das entsprechende Kästchen nicht markiert sein. Klicken Sie auf **Entfernen** um BitDefender von Ihrem Computer zu entfernen.



Wichtig

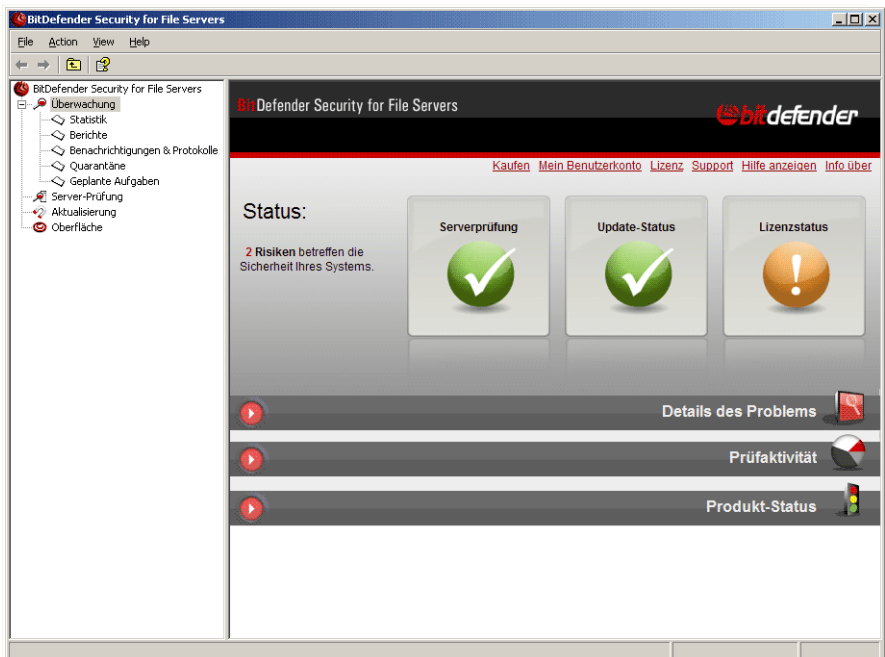
Dies wird alle BitDefender Produkte von Ihrem Computer entfernen. Wenn Sie zusätzliche BitDefender Produkte installiert haben und lediglich BitDefender Security for File Servers entfernen wollen, benutzen sie die **Modifizieren** Option.

Konfiguration und Verwaltung

6. Erste Schritte

BitDefender Security for File Server kann über eine zentrale MMC-basierte Management Konsole, konfiguriert und verwaltet werden. Die Management Konsole bietet Zugriff auf alle Funktionen und Einstellungen von BitDefender Security for File Server.

Sie erreichen die BitDefender Management-Konsole über das Windows-Startmenü: **Start → Programme → BitDefender Security for Windows Servers → BitDefender Security for File Server**. Schneller geht es jedoch mittels Doppelklick auf das **BitDefender Symbol** in der Systemleiste.



Konfiguration

Auf der linken Seite der Management-Konsole sehen Sie das Baummenu:

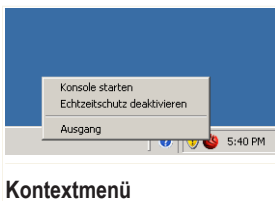
- **Überwachung** - zeigt das Dashboard an. Das Dashboard gibt Ihnen nützliche Informationen über den Status von BitDefender Security for File Server und hilft Ihnen dabei Probleme einfach zu lösen.
 - ☐ **Statistiken** - bietet einen statistischen Überblick über die Produktaktivität.
 - ☐ **Berichte** - dient zum Erstellen von benutzerdefinierten Berichten über die Produktaktivität.

- ☐ **Benachrichtigungen & Protokolle** - bietet die Möglichkeit die Protokolloptionen zu konfigurieren und Benachrichtigungen über die Ereignisse, die während des Betriebs des Produktes auftraten (wie ein Update-Fehler oder der Fund einer infizierten Datei), zu senden.
- ☐ **Quarantäne** - zeigt die Dateien an, die sich in der Quarantäne befinden. Diese Dateien wurden als infiziert oder verdächtig erkannt und wurden entsprechend der festgelegten Aktion in den Quarantäneordner verschoben.
- ☐ **Geplante Aufgaben** - dient zur Einrichtung zeitgesteuerter Aufgaben mithilfe eines hilfreichen Assistenten. Sie können Updates, On-Demand Prüfprozesse und die Erstellung von Berichten planen.
- **Server Scan** - BitDefender kann für die Prüfung des File Servers konfiguriert werden.
- **Update** - BitDefender kann aktualisiert und Update-Einstellungen können konfiguriert werden.
- **Allgemein** - BitDefender kann so konfiguriert werden, dass zu dem BitDefender Labor Berichte bezüglich der Viren gesendet werden, die auf dem Server gefunden wurden sowie über Vorfälle während des Produktbetriebs.

Wenn Sie die Hilfedatei öffnen möchten, klicken Sie auf **Hilfe -> Über BitDefender Security for File Server**. Für jedes Fenster steht eine Kontexthilfe zur Verfügung. Klicken Sie auf ? um diese zu öffnen.

6.1. BitDefender Symbol im Infobereich der Taskleiste

Wenn die Produktinstallation (einschließlich Neustart des Computers) abgeschlossen ist, wird in der Systemleiste ein Symbol angezeigt.



Bei einem Doppelklick auf dieses Symbol öffnet sich die Management-Konsole. Wird das Symbol mit der rechten Maustaste angeklickt, öffnet sich ein Kontextmenü mit dem Sie BitDefender schnell verwalten können.

- **Konsole starten** - dient zum Öffnen der Management-Konsole.
- **Echtzeitschutz Aktivieren/Deaktivieren** - dient zur Aktivierung/Deaktivierung des **Echtzeitschutzes**.
- **Beenden** - dient zum Beenden der Anwendung. Bei Auswahl dieser Option wird das entsprechende Systemleistsymbol ausgeblendet. Der Schutz durch BitDefender bleibt jedoch bestehen (vorausgesetzt, er wurde zuvor aktiviert).



Beachten Sie

In 3 Situationen färbt sich das Symbol grau:

- **Echtzeitschutz** ist deaktiviert.
- Der Service **BitDefender for File Server** ist gestoppt.
- Der Lizenzzeitraum ist abgelaufen.

Auf diese Weise werden Sie wissen ob BitDefender nicht in Betrieb ist ohne die Management-Konsole öffnen zu müssen.

Um das Taskleistsymbol für verschiedene Benutzerkategorien zu aktivieren/deaktivieren, öffnen Sie die Management-Konsole, und wählen Sie im Abschnitt **Allgemein** den Tab **Taskleistsymbol**.

6.2. Verbindung zu einem anderen Computer herstellen

Mit der Management-Konsole können Sie BitDefender Security for File Server Produkte ferngesteuert verwalten.



Wichtig

Um ein BitDefender Security for File Server Produkt ferngesteuert zu verwalten, müssen Sie zuerst ein **administratives Passwort** für das entsprechende Produkt einrichten. Bitte beachten Sie dass Sie, wenn Sie eine ferngesteuerte Verbindung zu BitDefender Security for File Server herstellen, nicht über alle Produktfunktionen verfügen. Sie können jedoch ein **Update auf Benutzeranfrage** durchführen und den **Echtzeitschutz** deaktivieren/aktivieren.

Um sich mit einem BitDefender Security for File Server Produkt, das auf einem Remotecomputer installiert ist, zu verbinden, befolgen Sie diese Schritte:

1. Klicken Sie mit der rechten Maustaste auf **BitDefender Security for File Server** im Baummenu.
2. Im Kontextmenu wählen Sie nun bitte **Mit einem anderen Computer verbinden**. Ein neues Fenster wird sich öffnen.



Mit einem anderen Computer verbinden.

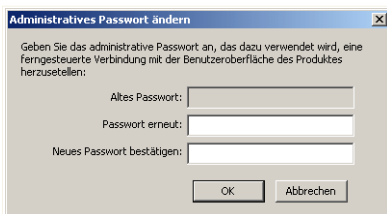
3. Geben Sie in das Feld **Mit einem anderen Computer verbinden** die IP-Adresse oder den Namen des Remotecomputers ein.
4. Geben Sie in das Feld **Passwort** das administrative Passwort für das entsprechende Produkt ein.
5. Klicken Sie auf **OK**.

6.3. Administratives Passwort ändern

Um BitDefender Security for File Server ferngesteuert zu verwalten, müssen Sie ein administratives Passwort einrichten. Für Benutzer mit limitierten Benutzerkonten ist ein administratives Passwort nötig, um auf BitDefender Security for File Servers durch Terminal Dienste zuzugreifen.

Um ein administratives Passwort einzurichten, befolgen Sie folgende Schritte:

1. Klicken Sie mit der rechten Maustaste auf **BitDefender Security for File Server** im Baummenu.
2. Im Kontextmenu wählen Sie bitte **Administratives Passwort ändern**. Ein neues Fenster wird sich öffnen.



Administratives Passwort ändern

3. Geben Sie in das Feld **Passwort** - das gewünschte administrative Passwort ein.
4. Geben Sie in das Feld **Passwort** - das gewünschte administrative Passwort ein.
5. Geben Sie in das Feld **Passwort bestätigen** - erneut das Passwort ein.
6. Klicken Sie auf **OK**.

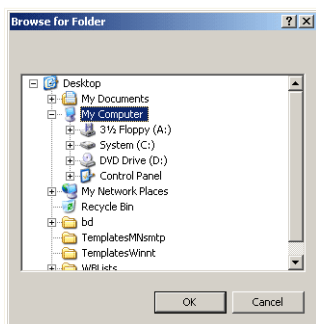
6.4. importieren/exportieren der Management Konsole Einstellungen

Sie können die Einstellungen der Management Konsole importieren und exportieren. Dies hilft Ihnen dabei, andere BitDefender Security for File Servers Produkte innerhalb des Netzwerks einfach zu konfigurieren und konfigurierte Einstellungen wiederherzustellen, falls Sie das Produkt reparieren oder neu installieren.

6.4.1. Policy-Einstellungen exportieren

Um die aktuellen Einstellungen der Konsole zu exportieren, befolgen Sie diese Schritte:

1. Klicken Sie mit der rechten Maustaste auf **BitDefender Security for File Server** im Baummenu.
2. Im Kontextmenu wählen Sie bitte **Konsole Einstellungen exportieren**.



Import-Tool

3. Wählen Sie den Ordner, in dem Sie die Produkteinstellungen speichern möchten und klicken Sie auf **OK**.

6.4.2. Policy-Einstellungen importieren

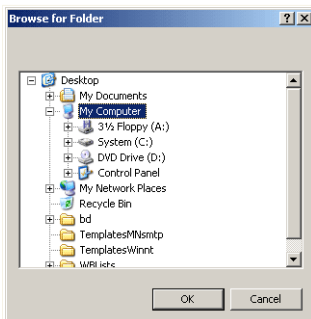
Um zuvor gespeicherte Konsoleeeinstellungen zu importieren, befolgen Sie diese Schritte:

1. Klicken Sie mit der rechten Maustaste auf **BitDefender Security for File Server** im Baummenu.
2. Im Kontextmenu wählen Sie bitte **Konsoleeeinstellungen importieren** um das Import Tool zu öffnen.



Import-Tool

3. Klicken Sie auf **Importieren**. Ein neues Fenster wird sich öffnen.



Import-Tool

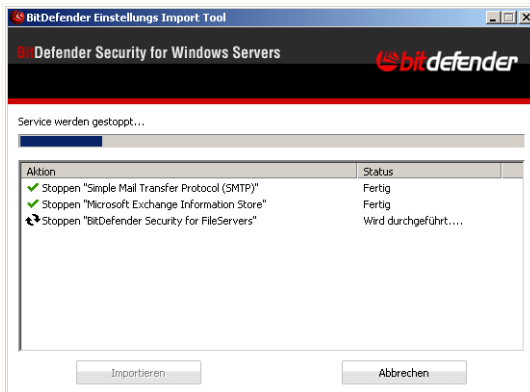
4. Wählen Sie den Ordner, in dem die Produkt Einstellungen gespeichert sind und klicken Sie auf **Weiter**, um diese zu importieren



Beachten Sie

Bemerken Sie bitte, dass BitDefender den Dateiserver nicht schützt, während Sie die Produkteinstellungen importieren. Deshalb wird es empfohlen, dass Sie den Dateiserver vom Netz vor dem Einleiten dieses Prozesses entfernen.

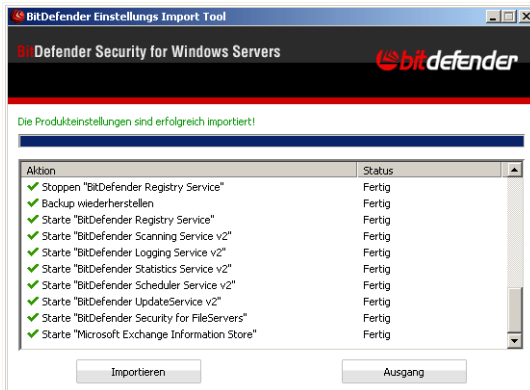
5. Warten Sie, bis das Import Tool den Importieren-Prozess vollendet.



Einstellungen importieren

Das Import-Tool zuerst die BitDefender Security for File Server-Dienstleistungen. Dann importiert es die Produkteinstellungen vom ausgewählten Ordner. Schließlich startet das Import-Tool die zuvor gestoppten Prozesse.

6. Sie werden vom Import Tool informiert sobald die Einstellungen erfolgreich importiert sind.



Fertigstellen

Klicken Sie auf **Ausgang**, um dieses Fenster zu schließen.

7. Registrierung und Mein Benutzerkonto

BitDefender Security for File Server verfügt über eine 30-tägige Testversion. Wenn Sie sich für BitDefender Security for File Server für Ihr Unternehmen entscheiden, registrieren Sie bitte die Vollversion. Sie sollten ein BitDefender Benutzerkonto registrieren, um sowohl den technischen Support als auch andere Serviceleistungen kostenlos nutzen zu können.

Öffnen Sie **Überwachung** im Baummenu um die Registrierung des Produktes und des Benutzerkontos durchzuführen.

- Klicken Sie auf **Registrieren** um BitDefender Security for File Servers zu registrieren, ein Benutzerkonto zu erstellen oder sich anzumelden, den Lizenzschlüssel zu ändern und um zu sehen wie viele Tage verbleiben, bis die Lizenz abläuft.
- Klicken Sie auf **Mein Benutzerkonto** wenn Sie sich nur an einem BitDefender Benutzerkonto anmelden oder es registrieren möchten.



Beachten Sie

Wenn BitDefender Security for File Server von dem BitDefender Management Server verwaltet wird, wird die Registrierung des Produktes und des Benutzerkontos über die Management Konsole des BitDefender Management Server durchgeführt.

7.1. Schritt 1/3 - BitDefender Security for File Server registrieren



Registrierung

Wenn Sie keine Bitdefender-Lizenz besitzen, klicken Sie auf den angegebenen Link, um zu dem BitDefender Online-Shop zu gelangen und einen Lizenzschlüssel zu erwerben.

Um BitDefender Security für File Servers zu registrieren, wählen Sie **Produkt registrieren**. Geben Sie den Lizenzschlüssel in das Feld **Lizenzschlüssel eingeben** ein und klicken Sie **Registrieren**.

Um das Produkt weiter zu testen, und wenn der Testzeitraum noch nicht beendet ist, klicken Sie bitte auf die Schaltfläche **Produkt weiter testen**. Sie können den aktuellen Lizenzschlüssel sehen und wann er abläuft.

Klicken Sie auf **Weiter**.



Beachten Sie

Falls der angegebene Lizenzschlüssel ungültig ist, werden Sie aufgefordert einen anderen Lizenzschlüssel einzugeben.

7.2. Schritt 2/3 - BitDefender Benutzerkonto registrieren

Mein Benutzerkonto

Bitte erstellen Sie einen BitDefender Konto, melden sich an Ihrem bestehenden Konto an, oder erstellen zu einem späteren Zeitpunkt ein Konto. Mit einem Konto können Sie immer mit BitDefender in Verbindung bleiben

☒ In ein existierendes Benutzerkonto einloggen

Nutzerkonto (E-Mail):

Kennwort:

[Kennwort vergessen?](#)

Sie haben kein Benutzerkonto oder Sie haben Ihre Anmeldeinformationen nicht eingegeben.

☐ Ein neues BitDefender Benutzerkonto erstellen

☐ Später ein Benutzerkonto erstellen

Registrierung des Benutzerkontos

Ich habe noch kein BitDefender-Benutzerkonto

Um ein BitDefender-Benutzerkonto zu erstellen, wählen Sie **Ein neues BitDefender Benutzerkonto erstellen** und geben Sie die benötigten Informationen ein. Die hier eingetragenen Daten bleiben vertraulich.



Beachten Sie

Wenn Sie dieses Konto später erstellen möchten, markieren Sie die entsprechenden Option.

- **E-Mail** - geben Sie Ihre E-Mail Adresse an.
- **Passwort** - geben Sie ein Passwort für Ihr BitDefender-Benutzerkonto ein. Das Passwort sollte mindestens 4 Zeichen haben.
- **Passwort erneut eingeben** - geben Sie erneut das vorher angegebene Passwort ein.
- **Vorname** - geben Sie Ihren Vornamen ein.
- **Name** - geben Sie Ihren Namen ein.



Beachten Sie

Benutzen Sie die angegebene E-Mail Adresse und das Passwort um sich in Ihr Benutzerkonto unter folgendem Link einzuloggen: <http://myaccount.bitdefender.com>.

Klicken Sie **Konto erstellen**.

Um erfolgreich ein Benutzerkonto einzurichten müssen Sie zunächst Ihre E-Mail Adresse aktivieren. Überprüfen Sie hierzu Ihre E-Mails unter der angegebenen Adresse und folgen Sie den Instruktionen, die Sie vom BitDefender Registrierungsservice zugesandt bekommen haben.

Klicken Sie auf **Weiter**.

Ich habe bereits ein BitDefender Benutzerkonto.

BitDefender weist Sie daraufhin, falls bereits ein BitDefender-Benutzerkonto auf Ihrem Computer registriert wurde. In diesem Fall müssen Sie nur auf **Weiter** klicken.

Wenn Sie bereits ein aktives Konto haben, BitDefender es jedoch nicht erkennt, wählen Sie **An einem bestehenden Konto anmelden**, geben Sie die E-Mail Adresse und das Passwort Ihres Kontos an und klicken Sie **Anmelden**.



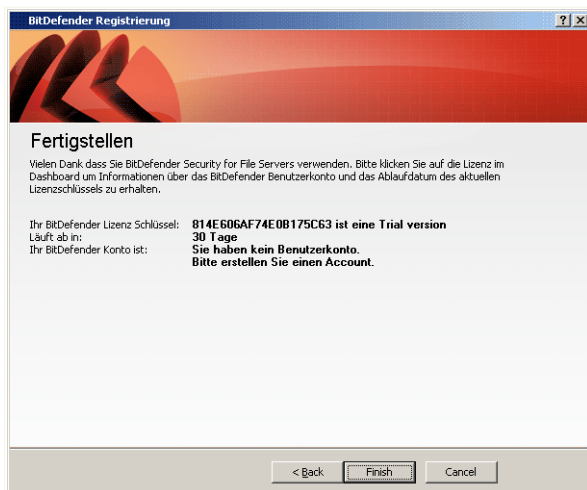
Beachten Sie

Wenn das angegebene Passwort nicht korrekt ist, so werden Sie dazu aufgefordert es erneut anzugeben, sobald Sie auf **Weiter** klicken. Klicken Sie auf **Ok** um das Passwort erneut einzugeben oder auf **Abbrechen** um den Assistent zu beenden.

Wenn Sie Ihr Passwort vergessen haben, klicken Sie **Passwort vergessen?** und folgen Sie den Instruktionen.

Klicken Sie auf **Weiter**.

7.3. Schritt 3/3 - Fertigstellen



Fertigstellen

Klicken Sie auf **Beenden**, um das Fenster zu schließen.



Beachten Sie

Um sich in Ihr BitDefender Benutzerkonto einzuloggen, klicken Sie auf **Mein Benutzerkonto**.

8. Überwachung

Der Überwachungsbereich bietet Ihnen alle nötigen Funktionen, um die Produktaktivität zu überwachen und zu kontrollieren.

Wenn Sie auf **Überwachung** im Baummenu klicken, wird das **Dashboard** angezeigt. Das Dashboard gibt Ihnen nützliche Informationen über den Status von BitDefender Security for File Server und hilft Ihnen dabei Probleme einfach zu lösen.

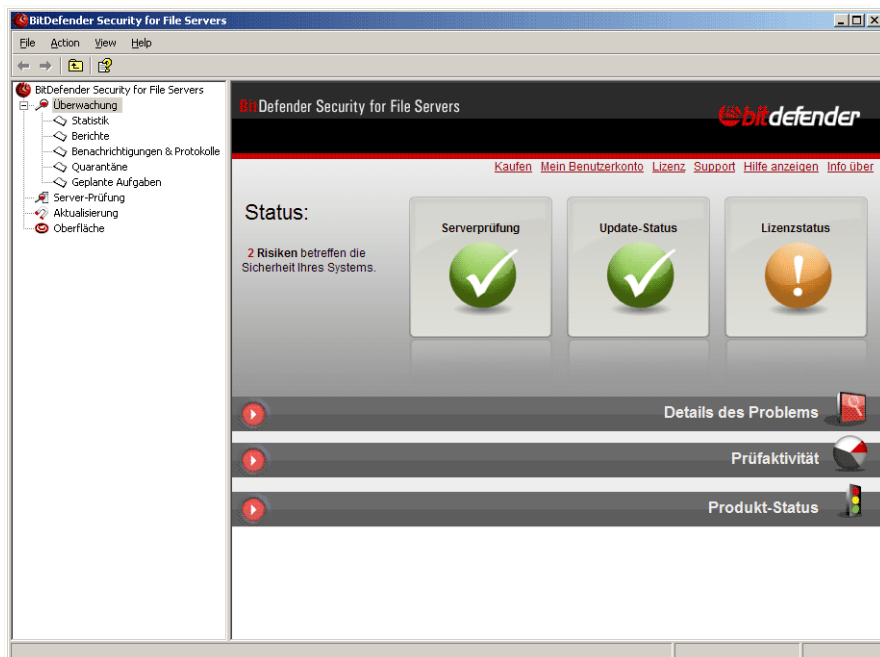
Unter dem Überwachungsbereich im Baummenu können Sie auf die folgenden Bereiche zugreifen:

- **Statistiken** - bietet einen statistischen Überblick über die Produktaktivität.
- **Berichte** - dient zum Erstellen von benutzerdefinierten Berichten über die Produktaktivität.
- **Benachrichtigungen & Protokolle** - bietet die Möglichkeit die Protokolloptionen zu konfigurieren und Benachrichtigungen über die Ereignisse, die während des Betriebs des Produktes auftraten (wie ein Update-Fehler oder der Fund einer infizierten Datei), zu senden.
- **Quarantäne** - zeigt die Dateien an, die sich in der Quarantäne befinden. Diese Dateien wurden als infiziert oder verdächtig erkannt und wurden entsprechend der festgelegten Aktion in den Quarantäneordner verschoben.
- **Geplante Aufgaben** - dient zur Einrichtung zeitgesteuerter Aufgaben mithilfe eines hilfreichen Assistenten. Sie können Updates, On-Demand Prüfprozesse und die Erstellung von Berichten planen.

In diesem Kapitel finden Sie eine detaillierte Beschreibung über jeden Bereich.

8.1. Dashboard

Klicken Sie auf **Überwachung** im Baummenu um das Dashboard zu sehen.



Dashboard

Das Dashboard gibt Ihnen nützliche Informationen über den Status von BitDefender Security for File Server und hilft Ihnen dabei Probleme einfach zu lösen. Sie sollten das Dashboard regelmäßig überprüfen, um Probleme, die die Sicherheit des File Server betreffen, schnell lösen zu können.

8.1.1. Wichtige Links

Im oberen Bereich des Dashboards befinden sich mehrere nützliche Links.

Link	Beschreibung
Kaufen	Öffnet eine Webseite auf der Sie das Produkt erwerben können.
Benutzerkonto	Öffnet Ihr BitDefender Benutzerkonto.
Registrieren	Öffnet den Registrierungsassistent
Support	Öffnet die BitDefender Support Webseite
Hilfe	Öffnet die Hilfedatei.
Über	Öffnet ein Fenster mit Details über das Produkt.

8.1.2. Statusbereich

Der Bereich **Status** beinhaltet Informationen über Probleme und hilft Ihnen, diese zu lösen.

Drei Statusschaltflächen, die drei Problemkategorien überwachen, informieren Sie direkt über das Vorhandensein bestimmter Probleme:

- **Server-Prüfung**
- **Update-Status**
- **Lizenz-Status**



Beachten Sie

Die Schaltfläche Lizenzstatus und die dazugehörigen Angelegenheiten sind nicht verfügbar, wenn BitDefender Security for File Server vom BitDefender Management Server verwaltet wird.

Auf der linken Seite der Statusschaltflächen können Sie die Anzahl der Probleme sehen, die die Sicherheit des File Servers betreffen (falls vorhanden).

Die Schaltflächen können je nach Sicherheitsstatus des File Servers die Farben grün, orange oder rot annehmen:

- Wenn die Status-Schaltflächen **Grün** aufleuchten, gibt es nichts, worüber Sie sich Sorgen machen müssten.
- **Gelb** signalisiert ein mittleres Sicherheitsrisiko für Ihren Computer. Diese Probleme verlangen zwar keine direkte Aufmerksamkeit, doch sollten Sie sich so bald wie möglich mit Ihnen befassen.
- Wenn die Status-Schaltflächen **Rot** aufleuchten, wird die Anwesenheit eines wichtigen Sicherheitsrisikos angezeigt, das Ihre direkte Aufmerksamkeit erfordert.

Befolgen Sie eine der folgenden Möglichkeiten, um Details über diese Risiken zu erfahren:

- Klicken Sie auf eine Statusschaltfläche um die entsprechende Problemkategorie zu sehen.
- Klicken Sie auf  entsprechend zu **Problem Details** um diesen Bereich zu erweitern und alle möglichen Probleme/Risiken zu sehen.

Der Bereich **Problem Details** beinhaltet drei Tabellen, eine für jede Statusschaltfläche. Jede Tabelle zeigt die überwachten Objekte und deren aktuellen Status an. Wenn ein Problem eines der überwachten Objekte betrifft, wird ein roter Link **Beheben** angezeigt. Klicken Sie entweder auf die **Beheben**-Schaltfläche, um ein Risiko nach dem anderen zu beheben oder verwenden Sie die Schaltfläche **Alle beheben** um alle auf einmal zu beheben.



Wichtig

Für jedes überwachte Objekt gibt es ein Kontrollkästchen, das in der Spalte **Überwachen** standardmäßig markiert ist. Wenn Sie möchten, dass ein bestimmtes Objekt nicht überwacht wird, deaktivieren Sie das entsprechende Kontrollkästchen.

Serverprüfung

Wenn die Schaltfläche für die Server-Prüfung rot oder orange ist, betreffen Probleme die Prüfkativität von BitDefender Security for File Server.

Klicken Sie auf die Schaltfläche um die entsprechenden Probleme zu sehen. Eine Tabelle mit dem Namen **Server-Prüfung** wird angezeigt und Sie können die überwachten Objekte und deren aktuellen Status sehen.

- **Echtzeitschutz.** Die Probleme, die angezeigt werden können sind in der folgenden Tabelle aufgeführt:

Status	Beschreibung
Dateien prüfen deaktiviert	Besonderes Risiko. Der Echtzeitschutz ist deaktiviert und der File Server ist nicht gegen Malware geschützt. Klicken Sie auf Beheben - um den Echtzeitschutz zu aktivieren.
Die Registrierung ist abgelaufen Fix	Besonderes Risiko. Der Lizenzzeitraum ist abgelaufen. Klicken Sie auf Beheben um den Registrierungsassistenten zu öffnen und BitDefender Security for File Server mit einem neuen Lizenzschlüssel zu registrieren.

Update Status

Wenn die Schaltfläche für den Update-Status orange oder rot ist, gibt es Angelegenheiten bezüglich des Updates die BitDefender Security for File Server betreffen.

Klicken Sie auf die Schaltfläche um die entsprechenden Probleme zu sehen. Eine Tabelle mit dem Namen **Update-Status** wird angezeigt und Sie sehen die überwachten Objekte und deren aktuellen Status.

- **Letztes signierte Aupdate.** Die Probleme, die angezeigt werden können sind in der folgenden Tabelle aufgeführt:

Status	Beschreibung
Mindestens eine Update-Location ist ausgefallen	Besonderes Risiko. Einen oder beide Update Orte konnten während des letzten Update Vorgangs nicht erreicht werden. Klicken Sie auf Beheben um ein neues Update zu starten.
Kein Update durchgeführt	Besonderes Risiko. Klicken Sie auf Beheben um ein neues Update zu starten. Der Status wechselt dann auf Lade herunter.
Update fehlgeschlagen, da die Updates auf Ihrem Server nicht signiert sind und Sie gewählt haben nicht signierte Updates nicht zu erlauben	Besonderes Risiko. Gehen Sie zu Update > Locations und markieren Sie Unsignierte Updates erlauben für Ihren Server.

- **Letzte Produktaktualisierung.** Die Probleme, die angezeigt werden können sind in der folgenden Tabelle aufgeführt:

Status	Beschreibung
Produktaktualisierung deaktiviert	Besonderes Risiko. Automatische Produktupdates sind deaktiviert. Dies macht Ihren Server angreifbarer für Sicherheitsbedrohungen. Klicken Sie auf Beheben um das automatische Update zu aktivieren.
Produktupdate wurde heruntergeladen, bitte installieren Sie es	Besonderes Risiko. Ein neues Produkt wurde heruntergeladen und noch nicht auf Ihrem System installiert. Klicken Sie auf Beheben, um das Update zu installieren. Wenn das Update ein anhalten des Serververkehrs oder einen Neustart verlangt, müssen Sie Ihre Auswahl bestätigen, indem Sie OK klicken. Um die Installation von verfügbaren Produktupdates zu planen, die ein Anhalten des Serververkehrs oder einen Neustart verlangen, klicken Sie statt dessen Alle Probleme beheben.

Status	Beschreibung
Ein neues Paket ist verfügbar und nicht auf Ihrem System installiert	Besonderes Risiko. Das neue Paket verfügt möglicherweise über neue Funktionen. Klicken Sie auf Beheben um das Paket zu installieren. Sie werden aufgefordert, Ihre Auswahl zu bestätigen. Klicken Sie dazu auf OK. Bitte beachten Sie, dass die Installation des Paketes einen Neustart des Servers erfordern kann.

- **Signatur Update älter als einen Tag.** Die Probleme, die angezeigt werden können sind in der folgenden Tabelle aufgeführt:

Status	Beschreibung
Updates sind alt	Besonderes Risiko. Mehr als ein Tag ist seit dem letzten Update vergangen Klicken Sie auf Beheben um ein neues Update zu starten. Der Status wechselt dann auf Lade herunter.

- **Automatisches Update.** Die Probleme, die angezeigt werden können sind in der folgenden Tabelle aufgeführt:

Status	Beschreibung
Automatisches Update ist deaktiviert und keine geplante Update-Aufgabe ist festgelegt oder aktiviert	Besonderes Risiko. BitDefender Security for File Server wird nicht automatisch regelmäßig aktualisiert. Klicken Sie auf Beheben um das automatische Update zu aktivieren. Wenn nicht anders konfiguriert, wird das Update-Intervall auf eine Stunde eingestellt.

Lizenzstatus

Wenn die Schaltfläche für den Lizenzstatus orange oder rot ist, existieren Angelegenheiten bezüglich der Lizenz Ihres BitDefender Security for File Server.



Beachten Sie

Die Schaltfläche Lizenzstatus und die dazugehörigen Angelegenheiten sind nicht verfügbar, wenn BitDefender Security for File Server vom BitDefender Management Server verwaltet wird. In diesem Fall wird die Registrierung von der Management-Konsole des BitDefender Management Server durchgeführt.

Klicken Sie auf die Schaltfläche um die entsprechenden Probleme zu sehen. Eine Tabelle mit dem Namen **Lizenzstatus** wird angezeigt und Sie können die überwachten Objekte und deren aktuellen Status sehen.

- **Registrierung.** Die Probleme, die angezeigt werden können sind in der folgenden Tabelle aufgeführt:

Status	Beschreibung
Sie benutzen eine Testversion des Produktes und sollten es registrieren	Erfordert Aufmerksamkeit. Der Status wird während der Testzeit angezeigt. Klicken Sie auf Beheben um den Registrierungsassistenten zu öffnen und BitDefender Security for File Server mit einem neuen Lizenzschlüssel zu registrieren.
Ihre Produktregistrierung wird in x Tagen ablaufen. Sie sollten Ihre Registrierung erneuern	Erfordert Aufmerksamkeit. Der Status wird während der letzten 30 Tage des Lizenzzeitraums angezeigt. Klicken Sie auf Beheben um den Registrierungsassistenten zu öffnen und BitDefender Security for File Server mit einem neuen Lizenzschlüssel zu registrieren.
Produktregistrierung abgelaufen. Sie sollten es registrieren	Besonderes Risiko. Der Lizenzzeitraum ist abgelaufen. Klicken Sie auf Beheben um den Registrierungsassistenten zu öffnen und BitDefender Security for File Server mit einem neuen Lizenzschlüssel zu registrieren.
Die Seriennummer, die Sie eingegeben haben, ist ungültig!	Erfordert Aufmerksamkeit. Sie haben einen ungültigen Lizenzschlüssel eingegeben. Klicken Sie auf Beheben um den Registrierungsassistenten zu öffnen und BitDefender Security for File Servers mit einem neuen Lizenzschlüssel zu registrieren.

- **Mein Benutzerkonto.** Die Probleme, die angezeigt werden können sind in der folgenden Tabelle aufgeführt:

Status	Beschreibung
Sie haben kein Benutzerkonto. Bitte erstellen Sie ein Konto.	Erfordert Aufmerksamkeit. Sie haben noch kein Benutzerkonto registriert. Klicken Sie auf Beheben um den Registrierungsassistent zu öffnen und ein neues

Status	Beschreibung
	Benutzerkonto zu erstellen oder Details zu einem Bestehenden anzugeben.
Das Passwort ist falsch. Versuchen Sie es erneut.	Klicken Sie auf Beheben um den Registrierungsassistenten zu öffnen und ein neues Benutzerkonto zu erstellen oder sich an einem bestehenden anzumelden.
Server Fehler. Bitte versuchen Sie es später nochmal	Erfordert Aufmerksamkeit. Eine Verbindung zum BitDefender Server konnte nicht hergestellt werden. Klicke Reparieren um den Registrierungsassistenten zu öffnen und versuchen Sie es nochmal.
Benutzerkonto gesperrt	Klicken Sie auf Beheben um den Registrierungsassistenten zu öffnen und ein neues Benutzerkonto zu erstellen oder sich an einem bestehenden anzumelden.

- **Benachrichtigung für Registrierung wird ablaufen.** Die Probleme, die angezeigt werden können sind in der folgenden Tabelle aufgeführt:

Status	Beschreibung
In x Tagen läuft Ihr Lizenzschlüssel ab.	Erfordert Aufmerksamkeit. Der Status wird während der letzten 30 Tage des Lizenzzeitraums angezeigt. Klicken Sie auf Beheben um den Registrierungsassistenten zu öffnen und BitDefender Security for File Server mit einem neuen Lizenzschlüssel zu registrieren.
Produkt abgelaufen	Besonderes Risiko. Der Lizenzzeitraum ist abgelaufen. Klicken Sie auf Beheben um den Registrierungsassistenten zu öffnen und BitDefender Security for File Server mit einem neuen Lizenzschlüssel zu registrieren.

8.1.3. Prüfkaktivität

Um grafische Statistiken über die Prüfkaktivität von BitDefender Security for File Server zu sehen, klicken Sie auf  entsprechend zu dem Bereich **Prüfkaktivität**.



Beachten Sie

Wenn Sie detaillierte Statistiken sehen möchten, klicken Sie auf **Statistiken** im Baummenu.

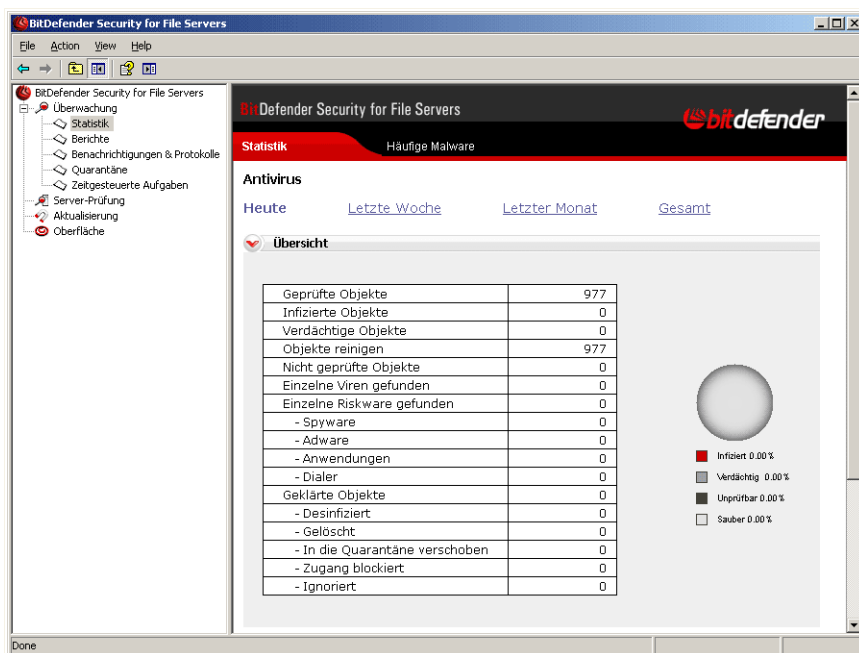
8.1.4. Produkt-Status

Um Informationen zu dem Produkt-Status zu sehen, klicken Sie auf  entsprechend zu dem Bereich **Produkt-Status**.

Sie können den Namen des Servers sehen, auf dem BitDefender Security for File Server installiert ist, sowie die Produktversion und die Anzahl der verfügbaren Malware-Signaturen.

8.2. Statistik

Wenn Sie detaillierte Statistiken über die Aktivität der Echtzeitprüfung von BitDefender Security for File Server sehen wollen, klicken sie auf **Statistiken** im Baummenu.



Statistik

BitDefender speichert Daten über die geprüften Objekte in Echtzeit auf eine Datenbank. Indem diese Datenbank verwendet wird, kann BitDefender detaillierte Statistiken liefern, mit denen Sie Folgendes einschätzen können:

- der Sicherheitsstatus des File Servers.
- die bestehenden Bedrohungen und deren Gefahrenpotenzial.

Folgende Arten von Statistiken stehen zur Verfügung:

Typ	Beschreibung
Zusammenfassung	Bietet allgemeine Statistiken über die Prüfkaktivität in Echtzeit von BitDefender Security for File Server: • Anzahl der geprüften Objekte. • Anzahl der gefundenen infizierten/verdächtigen/sauberen Objekte. • Anzahl der Objekte, die nicht geprüft werden konnten. • Anzahl der entdeckten Viren. • Anzahl der entdeckten Riskware, sowohl insgesamt als auch nach Riskware-Typ geordnet. • Anzahl der gelösten Probleme, sowohl insgesamt als auch nach Aktionstyp geordnet. Ein Kreisdiagramm zeigt die Prozentzahl infizierter, verdächtiger, nicht prüfbarer und sauberer Dateien an. Gemeinsam stellen diese die gesamte Anzahl der geprüften Dateien dar.
Top Malware	Zeigt die 10 am häufigsten entdeckten Malwares. Klicken Sie auf den Tab Malware um diese Statistiken anzuschauen.

Die Statistiken sind in 4 Zeitintervalle unterteilt: heute, letzte Woche, letzter Monat und insgesamt. Um Statistiken zu öffnen klicken Sie auf den entsprechenden Link.



Beachten Sie

Die Statistiken werden alle 60 Sekunden aktualisiert um Sie mit Informationen in Echtzeit zu versorgen.

8.2.1. Statistiken säubern

Standardmäßig löscht BitDefender statistische Informationen, die älter als 30 Tage sind. Sie können die Säuberungsoptionen im unteren Bereich des Abschnitts **Statistiken** konfigurieren. Geben Sie in das Editierfeld die Anzahl der Tage/Wochen/Monate ein, die die Informationen gespeichert werden sollen.

Wenn Sie die Statistiken manuell säubern möchten, klicken Sie mit der rechten Maustaste auf **Statistiken** im Baummenu. Klicken Sie anschließend auf die Option **Alle Statistiken säubern**.



Beachten Sie

Bitte beachten Sie, dass Berichte und Statistiken mithilfe der gleichen Datenbank erstellt werden. Das Säubern der Statistiken hat also auch Auswirkungen auf die Genauigkeit der Berichte.

8.3. Berichte

Mit BitDefender können Berichte über die Prüfkaktivität in einen bestimmten Zeitraum erstellt werden. Diese Berichte können sehr nützlich sein, sie können ausgedruckt und an Andere weitergesendet werden, die sich für den Status der Sicherheit des File Servers interessieren.

Berichte können im HTML- oder im CSV-Format erstellt werden. Folgende Berichtstypen können erstellt werden:

Berichtstyp	Beschreibung
Gesamt	Bietet umfangreiche Informationen über die Bedrohungen die innerhalb eines bestimmten Zeitraums entdeckt wurden.
Häufigste Viren	Bietet eine Tabelle mit den entdeckten Bedrohungen, die innerhalb eines bestimmten Zeitraums entdeckt wurden, geordnet nach der Anzahl der infizierten Dateien.

Die Berichte sind im Ordner `C:\Programdateien\BitDefender\BitDefender Security for File Server\Berichte` gespeichert.



Beachten Sie

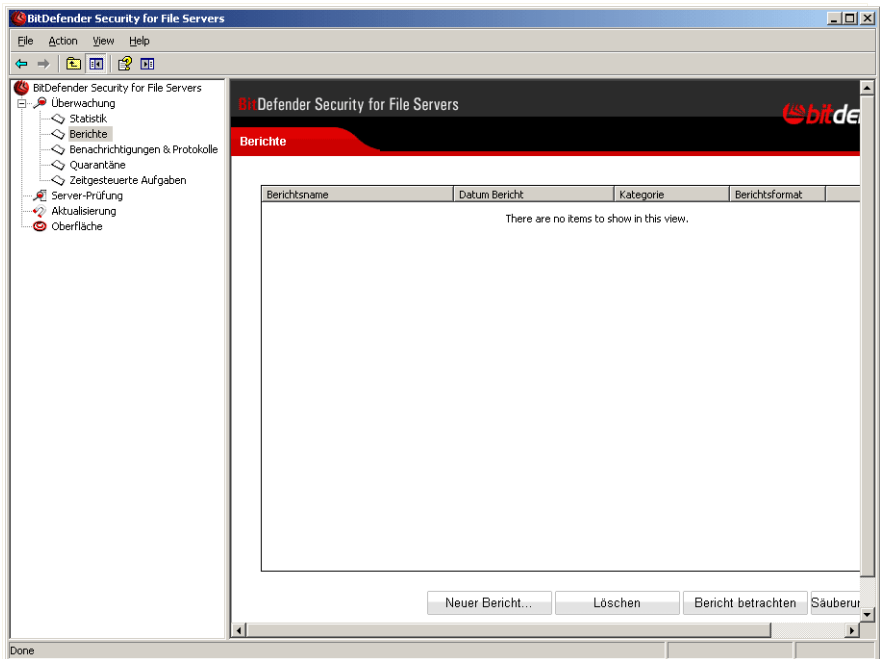
Berichte werden anhand der Informationen erstellt, die sich in der **BitDefender Datenbank** befinden, die standardmäßig einmal pro Woche gesäubert wird. Wenn Berichte während des Zeitraums gelöscht werden, die vom Bericht selbst abgedeckt werden, so können die gelieferten Informationen ungenau sein.

Um Berichte zu erstellen, zu betrachten und zu verwalten, klicken Sie auf **Berichte** im Baummenu (unter **Überwachen**).



Wichtig

In dem Bereich **Berichte** finden Sie auch die On-Demand Prüfberichte.



Berichte

Sie können alle existierenden Berichte in der Tabelle aufgelistet sehen. Für jeden Bericht werden folgende Informationen angezeigt: Name des Berichts, Datum der Erstellung des Berichts, die Art der beinhalteten Informationen und das Format.

8.3.1. Berichte verwalten

Verwenden Sie die zur Verfügung stehenden Schaltflächen um Berichte zu verwalten.

- **Neuer Bericht** - startet den Assistenten, der Ihnen beim Erstellen eines neuen Berichtes hilft.
- **Löschen** - löscht einen oder mehrere ausgewählte Berichte. Sie werden aufgefordert, Ihre Auswahl zu bestätigen. Klicken Sie dazu auf **Ja**.
- **Bericht anzeigen** - öffnet den ausgewählten Bericht.



Beachten Sie

Sie können den Bericht auch mit einem Doppelklick öffnen.

- **Säuberungsoptionen** - öffnet ein Fenster, in welchem Sie festlegen können wie lange die Berichte aufbewahrt werden sollen. Geben Sie die Anzahl der Stunden /

Tage / Wochen / Monate für die Aufbewahrung ein und klicken Sie auf **OK** um die Änderungen zu speichern.



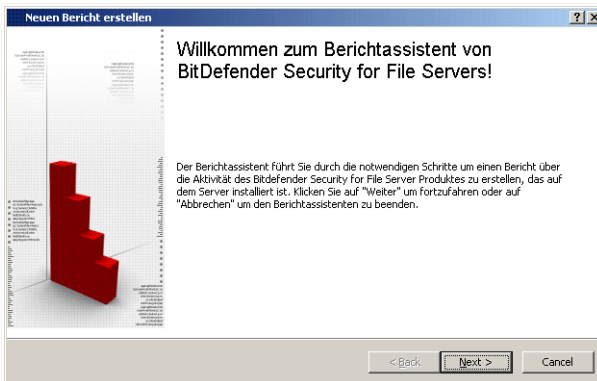
Beachten Sie

Berichte, die älter als der angegebene Zeitraum sind, werden automatisch gelöscht.

8.3.2. Berichte erstellen

Um Berichte über die Produktaktivität zu erstellen, klicken Sie auf **Neuer Bericht** und führen Sie den Assistenten durch.

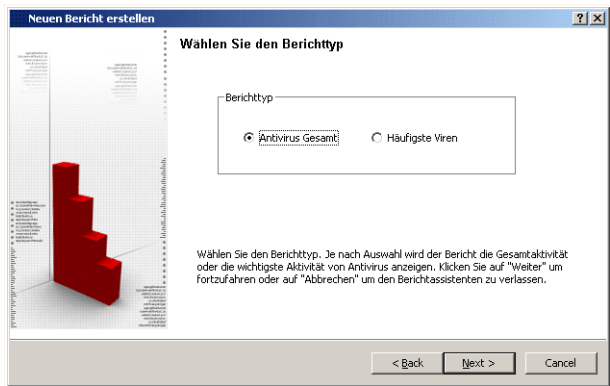
Schritt 1/5 - Willkommen beim Berichtsassistenten.



Willkommen

Klicken Sie auf **Weiter**.

Schritt 2/5 – Berichtstyp wählen



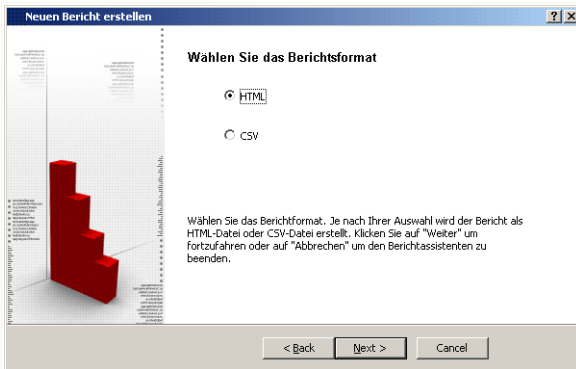
Wählen Sie den Berichtstyp

Wählen Sie eine der zur Verfügung stehenden Berichtstypen.

Berichtstyp	Beschreibung
Gesamt	Bietet umfangreiche Informationen über die Bedrohungen die innerhalb eines bestimmten Zeitraums entdeckt wurden.
Häufigste Viren	Bietet eine Tabelle mit den entdeckten Bedrohungen, die innerhalb eines bestimmten Zeitraums entdeckt wurden, geordnet nach der Anzahl der infizierten Dateien.

Klicken Sie auf **Weiter**.

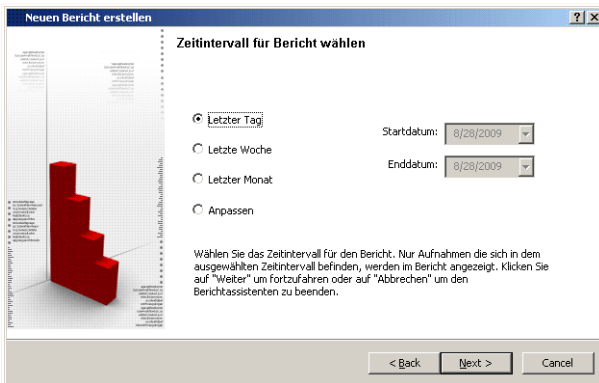
Schritt 3/5 – Berichtsformat wählen



Wählen Sie das Berichtsformat

Wählen Sie das Format der Berichtdatei (**HTML** oder **CSV**).
Klicken Sie auf **Weiter**.

Schritt 4/5 – Zeitraum auswählen



Wählen Sie den Zeitraum aus

Wählen Sie den im Bericht bedeckten Zeitabstand aus:

- **Letzter Tag**
- **Letzte Woche**
- **Letzter Monat**
- **Benutzerdefiniert**

Wenn Sie Information über BitDefender mit einem spezifischen Zeitabstand verbundene Tätigkeit benötigen, wählen Sie **anpassen** und geben Sie das Beginn/Endedatum an. Um das Startdatum und das Ende festzulegen, klicken Sie entweder auf die Datumsfelder und geben Sie neue Werte ein oder klicken Sie auf **den Pfeil** um ein Datum aus dem Kalender zu wählen.



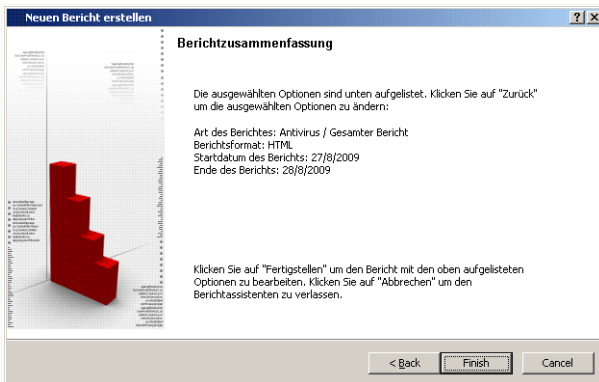
Beachten Sie

Das Format des Datums ist Monat/Tag/Jahr.

Nur Aufnahmen aus dem festgelegten Zeitraum werden in dem Bericht erscheinen.

Klicken Sie auf **Weiter**.

Schritt 5/5 – Zusammenfassung betrachten



Betrachten Sie die Zusammenfassung

In diesem Fenster können Sie die getätigten Berichtseinstellungen überprüfen. Sie können Änderungen vornehmen, indem Sie zu den vorherigen Schritten zurückkehren (klicken Sie auf **Zurück**).

Klicken Sie auf **Beenden**, um den Bericht zu erstellen. Der Bericht wird nun im Bereich **Berichte** angezeigt.

8.4. Benachrichtigungen & Protokolle

Mit Benachrichtigungen & Protokolle können Sie das Benachrichtigungssystem von BitDefender konfigurieren.

BitDefender ist standardmäßig so konfiguriert, dass die Aktivität protokolliert wird. Das BitDefender Protokoll liefert Ihnen eine umfangreiche Liste der Ereignisse, die während des Produktbetriebs aufgetreten sind. Um die Protokollierung zu konfigurieren oder die Protokolldateien zu betrachten, öffnen Sie den Tab **Protokollierung**.

Weiterhin können Sie Bitdefender so konfigurieren, dass bestimmte Benutzer sofort benachrichtigt werden, wenn bestimmte Ereignisse während des Produktbetriebs auftreten. Benachrichtigungen können mit dem Befehl `Net Send` gesendet werden. Um die Mail- und Net Send Benachrichtigungsdienste zu konfigurieren, öffnen Sie den Tab **Benachrichtigungen**.



Beachten Sie

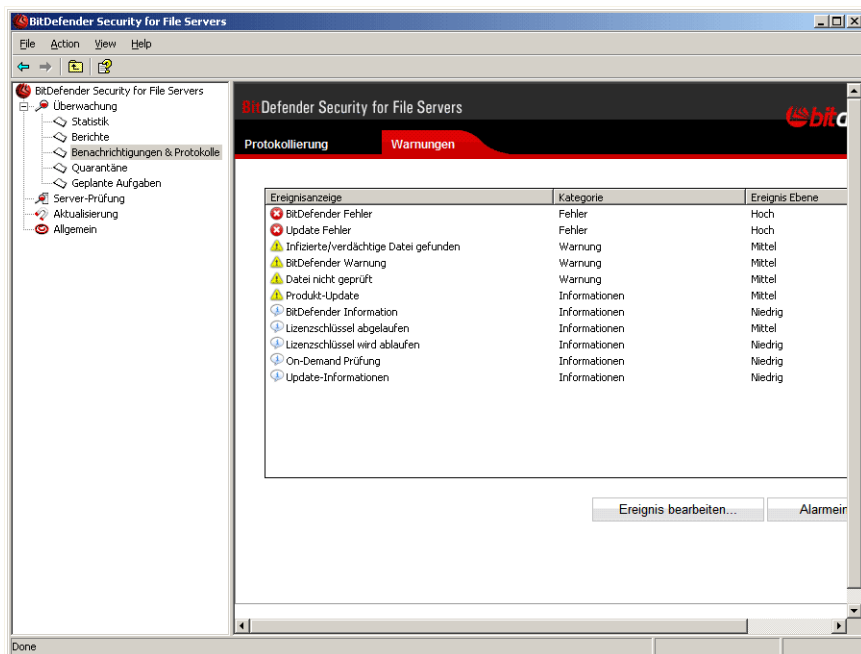
Bemerken Sie bitte, daß Windows Server 2008 keine Unterstützung für Net Send Alarmsignale zur Verfügung stellt.

Der Tab **Benachrichtigungen** liefert Ihnen eine umfangreiche Liste der Ereignisse, die während des Produktbetriebs aufgetreten sind. Sie können Benachrichtigungen für jedes Ereignis vollständig deaktivieren oder Sie können BitDefender so konfigurieren, dass Mail- und Net Send Benachrichtigungen gesendet werden, wenn das Ereignis auftritt. Weitere Informationen finden Sie hier: „*Ereignisbenachrichtigung konfigurieren*“ (S. 53).

8.4.1. Benachrichtigungen

Benachrichtigungen sind Nachrichten, die produktbezogene Informationen beinhalten und die Empfänger über die Produktaktivität informieren sollen. BitDefender kann so eingestellt werden, dass Benutzer und Administratoren über Mail oder Net Send über auftretende Ereignisse benachrichtigt werden.

Um die Benachrichtigungsdienste und die Ereignisse über die Sie informiert werden möchten zu konfigurieren, klicken Sie auf **Benachrichtigungen & Protokolle** im Baummenu (unter **Überwachung**) und dann auf den Tab **Benachrichtigungen**.



Benachrichtigungen

Alle möglichen Ereignisse sind in der Tabelle aufgelistet. Es gibt 3 mögliche Ereignisse:

- **Information** - diese Ereignisse liefern Informationen über die Produktaktivität.
- **Warnung** - diese Ereignisse liefern wichtige Informationen über die Produktaktivität und erfordern Ihre Aufmerksamkeit.
- **Fehler** - diese Ereignisse liefern Informationen über Fehler die während des Produktbetriebs aufgetreten sind.

Hier ist die Liste der Ereignisse die auftreten können:

Ereignis	Beschreibung
BitDefender Fehler	Unterteilt alle Fehler, die während des Produktbetriebs auftreten können, so wie das Fehlschlagen des Starts.
Update-Fehler	Informiert über das Auftreten eines Fehlers während des Update-Prozesses.
Infizierte/verdächtige Datei entdeckt	Erscheint, wenn eine infizierte oder verdächtige Datei entdeckt wurde.

Ereignis	Beschreibung
BitDefender Warnung	Unterteilt wichtige Informationen über die Aktivität von BitDefender.
Datei nicht geprüft	Erscheint wenn eine Datei nicht von Bitdefender geprüft werden konnte.
BitDefender Information	Enthält Informationen über die Aktivität von BitDefender.
Lizenzschlüssel abgelaufen	Zeigt den Ablauf des Registrierungszeitraums an.
Lizenzschlüssel wird ablaufen	Zeigt an, dass noch 3 Tage verbleiben, bis die Lizenz abläuft.
On-Demand Prüfung	Erscheint wenn eine On-Demand Prüfung durchgeführt wird.
Update-Information	Enthält Informationen über den Update-Prozess.
Produkt-Update	Erscheint wenn ein Update zur Verfügung steht.

Benachrichtigungsdienst konfigurieren

Um den Benachrichtigungsdienst und die entsprechenden Einstellungen zu konfigurieren klicken Sie auf **Allgemeine Benachrichtigungseinstellungen**. Das Konfigurationsfenster wird erscheinen.

Mail-Alarme

BitDefender kann den Netzwerkadministrator durch das Senden konfigurierbarer Benachrichtigungen benachrichtigen, wenn ein Ereignis auftritt, für das diese eingestellt wurden. Durch die Aktivierung dieser Funktion erhalten Sie zeitnah wichtige Informationen zum Zustand Ihres Servers. Anhand dieser Informationen können Sie entscheiden, ob Sie über die Management-Konsole weitere Maßnahmen ergreifen müssen.



Beachten Sie

Dieses Modul integriert mit einem SMTP Server. Es arbeitet gut mit einem ESMTP Server, benutzt aber nicht das ESMTP Protokoll weil es auf SMTP implementiert ist.

Klicken Sie auf den Tab **Mail-Benachrichtigungen** um die Mail-Benachrichtigungsdienst zu konfigurieren.

Gemeinsame Benachrichtigungseinstellungen

Mail-Benachrichtigung | Net Send

☐ Mail-Alarm aktivieren

SMTP Mail-Benachrichtigungen
Geben Sie die SMTP Server-IP und den E-Mail-Absender an, die für das Versenden der Mail-Benachrichtigungen verwendet werden:

SMTP Server: 127.0.0.1

Von Adresse: BitDefender

☐ Benutze SMTP Server Authentifizierung

SMTP Benutzername:

SMTP Passwort:

Allgemeine Empfänger
Geben Sie die Empfänger für die Benachrichtigungen an. Klicken Sie auf das Eingabefeld und starten Sie mit der Eingabe, wobei Sie jeden Benutzernamen mit der Eingabetaste, einem Komma oder einem Strichpunkt trennen. Sie können auch mit Kopieren/Einfügen arbeiten oder sie aus einer Textdatei importieren.

Importieren... Exportieren...

OK Cancel Apply

Mail-Alarme

Um den Mail-Benachrichtigungsdienst zu nutzen, muss wie folgt vorgegangen werden:

1. Wählen Sie **Mail-Benachrichtigungen aktivieren** um den Mail-Benachrichtigungsdienst zu aktivieren.
2. Legen Sie die benötigten SMTP-Einstellungen fest um Mail-Benachrichtigungen zu senden.
 - **SMTP-Server** - geben Sie die IP-Adresse des SMTP-Servers ein, der in Ihrem Netzwerk zum Versenden von Nachrichten verwendet wird.
 - **Von Adresse** - geben Sie die E-Mail-Adresse ein, die im Absenderfeld angezeigt werden soll.



Wichtig

Sie müssen eine für den SMTP-Server gültige E-Mail-Adresse eintragen, da sonst der Fall eintreten kann, dass der Server Nachrichten von einem unbekannten Absender nicht weiterleitet.

3. Wenn der SMTP Server, der benutzt wird um Nachrichten zu versenden, authentifizierung benötigt, wählen Sie **Benutze SMTP Server Authentifizierung** und geben Sie den Benutzernamen und Passwort in die entsprechenden Felder ein.



Beachten Sie

NTLM Authentifizierung ist nicht unterstützt.

4. Legen Sie die Empfänger der Mail-Benachrichtigungen fest.
 - Geben Sie in das Editierfeld die E-Mail-Adressen der Empfänger der Mail-Benachrichtigungen an.
 - Um eine E-Mail-Adresse aus einer `txt` Datei zu importieren, klicken Sie auf **Importieren**, wählen Sie die Datei aus und klicken Sie dann auf **Öffnen**. Sie können die E-Mail Adressen auch aus der Textdatei kopieren und in das Editierfeld einfügen.
5. Klicken Sie anschließend auf **Anwenden** und **OK**, um die Einstellungen zu übernehmen und das entsprechende Fenster zu schließen.
6. Konfigurieren Sie die Ereignisse für die Mail-Benachrichtigungen gesendet werden sollen.

Um die vorhandenen Liste der E-Mail-Adressen in eine `txt` Datei zu exportieren, klicken Sie auf **Exportieren** und speichern Sie die Datei an dem gewünschten Ort.



Beachten Sie

Die hier festgelegten Empfänger werden bei Eintritt eines Ereignisses, für das dieser Benachrichtigungstyp eingestellt wurde, benachrichtigt. Um verschiedene Empfänger für jedes Ereignis festzulegen, öffnen Sie den Tab **Benachrichtigungen** und konfigurieren Sie die Ereignisse. Weitere Informationen finden Sie hier: „*Ereignisbenachrichtigung konfigurieren*“ (S. 53).

Wenn Sie diesen Dienst deaktivieren möchten, lassen Sie das Kontrollkästchen neben **Mail-Benachrichtigungen aktivieren** frei und klicken Sie auf **Anwenden** um die Änderungen zu speichern.

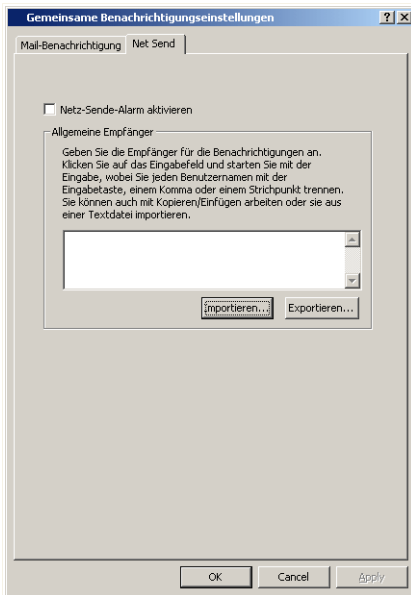
Net Send-Benachrichtigung

BitDefender kann den Netzwerkadministrator durch das Senden konfigurierbarer Benachrichtigungen über `Net Send` benachrichtigen, wenn ein Ereignis auftritt, für das diese eingestellt wurden.



Beachten Sie

Dieses Modul arbeitet mit dem Befehl `Net Send` des Windows-Betriebssystems, auf dem das Programm installiert ist. Die Alarmmeldungen beziehen sich auf die Aktivität des Produkts. Damit solche Alarmmeldungen empfangen werden können, muss der Administrator Nachrichten- und Alarmdienst auf dem Server und auf der Client-Arbeitsstation aktivieren. Windows Server 2008 unterstützt keine `Net Send` Benachrichtigungen.



Net Send-Benachrichtigung

Um den Net Send Benachrichtigungsdienst zu nutzen, muss wie folgt vorgegangen werden:

1. Wählen Sie **Net Send-Benachrichtigung aktivieren**, um den Net Send-Benachrichtigungsdienst zu aktivieren.
2. Geben Sie die Empfänger der Net Send-Benachrichtigungen an.
 - Geben Sie in das Editierfeld die Computernamen der Empfänger der Mail-Benachrichtigungen ein.
 - Um Computernamen aus einer `txt` Datei zu importieren, klicken Sie auf **Importieren**, wählen Sie die Datei aus und klicken Sie dann auf **Öffnen**. Sie können die Computernamen auch aus der Textdatei kopieren, und sie in das Editierfeld einfügen.
3. Klicken Sie anschließend auf **Anwenden** und **OK**, um die Einstellungen zu übernehmen und das entsprechende Fenster zu schließen.
4. Konfigurieren Sie die Ereignisse, für die Net Send Benachrichtigungen gesendet werden sollen, wie in dem Bereich „*Ereignisbenachrichtigung konfigurieren*“ (S. 53) beschrieben.



Beachten Sie

Die hier festgelegten Empfänger werden bei Eintritt eines Ereignisses, für das dieser Benachrichtigungstyp eingestellt wurde, benachrichtigt. Um verschiedene Empfänger

für jedes Ereignis festzulegen, öffnen Sie den Tab **Benachrichtigungen** und konfigurieren Sie die Ereignisse. Weitere Informationen finden Sie hier: „*Ereignisbenachrichtigung konfigurieren*“ (S. 53).

Um eine Liste in eine `txt` Datei zu exportieren, klicken Sie auf **Exportieren** und speichern Sie die Datei an dem gewünschten Ort.

Wenn Sie diesen Dienst deaktivieren möchten, lassen Sie das Kontrollkästchen neben **Net Send Benachrichtigungen aktivieren** frei und klicken Sie auf **Anwenden** um die Änderungen zu speichern.



Wichtig

Es ist nicht ratsam, diese Alarmart bei einem Virenausbruch zu verwenden.

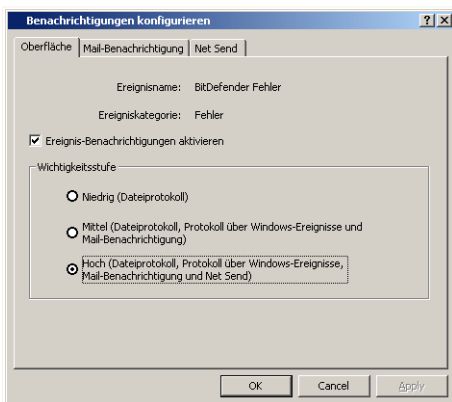
Ereignisbenachrichtigung konfigurieren

Sie können die Benachrichtigungsmethoden für jedes Ereignis in der Liste separat konfigurieren. Um die Benachrichtigungsmethoden für ein spezielles Ereignis zu konfigurieren, wählen Sie es aus und klicken Sie auf **Ereignis konfigurieren**. Das Konfigurationsfenster wird erscheinen.

Befolgen Sie diese Schritte um die Ereignisbenachrichtigung zu konfigurieren:

Schritt 1/3 - Wählen Sie die Ereigniswichtigkeit

Öffnen Sie das Konfigurationsfenster um die Wichtigkeit des Ereignisse auszuwählen.



Ereigniswichtigkeit auswählen

Der Name und die Kategorie des Ereignisses werden Ihnen angezeigt.

Standardmäßig ist die Ereignisbenachrichtigung für jedes auftauchende Ereignis aktiviert. Um die Ereignisbenachrichtigung zu deaktivieren, lassen Sie das Kontrollkästchen **Ereignisbenachrichtigung aktivieren** frei.



Beachten Sie

Wenn die Ereignisbenachrichtigung deaktiviert ist, wird das Ereignis nicht protokolliert und keine Benachrichtigung wird gesendet.

Wenn ein Ereignis stattfindet, kann es basierend auf seiner Wichtigkeit protokolliert werden und festgelegte Empfänger können über Mail- oder Net Send Benachrichtigungen über sein Auftreten informiert werden. Wählen Sie eine der folgenden Optionen um die Wichtigkeitsstufe einzustellen:

- **Niedrig (Dateiprotokoll)** - um das Ereignis in einer Protokolldatei aufzuzeichnen. Es wird keine Benachrichtigung gesendet, wenn das Ereignis stattfindet.
- **Mittel (Dateiprotokoll und SMTP)** - um das Ereignis zu protokollieren und Mail-Benachrichtigungen zu senden, wenn das Ereignis stattfindet.
- **Hoch (Dateiprotokoll, SMTP und Net Send)** - um das Ereignis zu protokollieren und Mail- und Net Send Benachrichtigungen zu senden, wenn das Ereignis stattfindet.



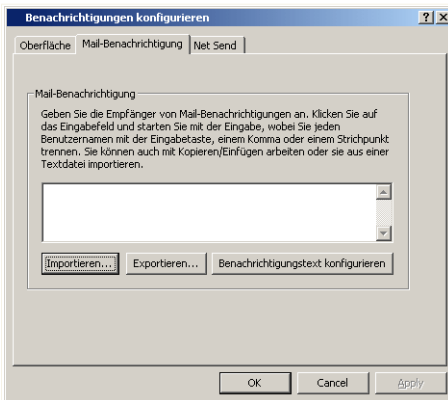
Beachten Sie

Um sicherzugehen, dass der Protokollierungsdienst und die Mail- und Net Send Benachrichtigung aktiviert ist, öffnen Sie die Bereiche **Protokolle** und **Benachrichtigungen**.

Klicken auf **Anwenden** und **OK**, um die Einstellungen zu übernehmen und das entsprechende Fenster zu schließen.

Schritt 2/3 – Mail-Benachrichtigungen konfigurieren

Wenn die Wichtigkeit des Ereignisses mittel oder hoch ist, werden Mail-Benachrichtigungen gesendet. Klicken Sie auf den Tab **Mail-Benachrichtigungen** um die Empfänger und den Text der Mail-Benachrichtigungen zu konfigurieren.



Mail-Benachrichtigungen konfigurieren

Mail-Benachrichtigungen werden zu den E-Mail-Adressen gesendet, die in dem Feld aufgelistet sind.



Beachten Sie

Zusätzlich zu diesen Empfängern werden die Mail-Benachrichtigungen auch zu den allgemeinen Benachrichtigungsempfängern gesendet. Für weitere Informationen lesen Sie bitte „Mail-Alarme“ (S. 49).

Benachrichtigungsempfänger konfigurieren

Um die Empfänger der Mail-Benachrichtigungen festzulegen:

- Geben Sie in das Editierfeld die E-Mail-Adressen der Empfänger der Mail-Benachrichtigungen ein.
- Um eine E-Mail-Adresse aus einer `txt` Datei zu importieren, klicken Sie auf **Importieren**, wählen Sie die Datei aus und klicken Sie dann auf **Öffnen**. Sie können die E-Mail Adressen auch aus der Textdatei kopieren und in das Editierfeld einfügen.

Wenn Sie die Liste in eine `txt` Datei exportieren möchten, klicken Sie auf **Exportieren** und speichern Sie die Datei an dem gewünschten Ort.

Konfigurieren Sie den Benachrichtigungstext.

Mail-Benachrichtigungen verfügen über einen Standardtext, der je nach Ereignis unterschiedlich ist.

Um den Standardtext zu sehen, klicken Sie auf **Benachrichtigungstext konfigurieren**.

Führen Sie die gewünschten Änderungen für den Inhalt der Benachrichtigung durch.



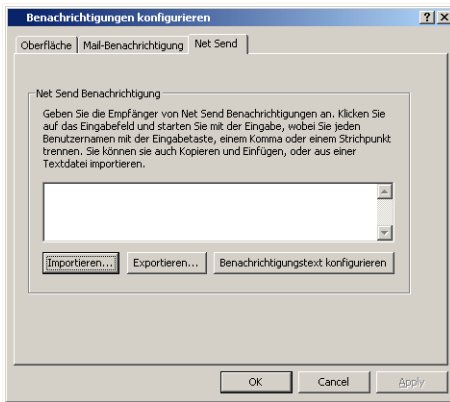
Wichtig

Sie sollten die Zeichenfolgen, die mit dem Symbol \$ beginnen nicht verändern, da diese wichtige Informationen über das Ereignis liefern.

Klicken auf **Anwenden** und **OK**, um die Einstellungen zu übernehmen und das entsprechende Fenster zu schließen.

Schritt 3/3 – Net Send Benachrichtigungen konfigurieren

Wenn die Wichtigkeit des Ereignisses hoch ist, werden Net Send Benachrichtigungen gesendet. Klicken Sie auf den Tab **Net Send Benachrichtigungen** um die Empfänger und den Text der Net Send Benachrichtigungen zu konfigurieren.



Net Send Benachrichtigungen konfigurieren

Net Send Benachrichtigungen werden zu den Computern gesendet, die in dem Feld aufgelistet sind.

Benachrichtigungsempfänger konfigurieren

Um die Empfänger der Net Send Benachrichtigungen festzulegen:

- Geben Sie die Computernamen der Empfänger in das Editierfeld ein.
- Um Computernamen aus einer `txt` Datei zu importieren, klicken Sie auf **Importieren**, wählen Sie die Datei aus und klicken Sie dann auf **Öffnen**. Sie können die Computernamen auch aus der Textdatei kopieren, und sie in das Editierfeld einfügen.

Wenn Sie die Liste in eine `txt` Datei exportieren möchten, klicken Sie auf **Exportieren** und speichern Sie die Datei an dem gewünschten Ort.



Beachten Sie

Neben den hier festgelegten Empfängern werde, die Benachrichtigungen auch zu all denen gesendet, die sich im Bereich **Benachrichtigungen** befinden (siehe „*Net Send-Benachrichtigung*“ (S. 51)).

Konfigurieren Sie den Benachrichtigungstext.

Net Send Benachrichtigungen verfügen über einen Standardtext, der je nach Ereignis unterschiedlich ist.

Um den Standardtext zu sehen, klicken Sie auf **Benachrichtigungstext konfigurieren**.

Führen Sie die gewünschten Änderungen für den Inhalt der Benachrichtigung durch.



Wichtig

Sie sollten die Zeichenfolgen, die mit dem Symbol \$ beginnen nicht verändern, da diese wichtige Informationen über das Ereignis liefern.

Klicken Sie anschließend auf **Anwenden** und **OK**, um die Einstellungen zu übernehmen und das entsprechende Fenster zu schließen.

8.4.2. Protokolle

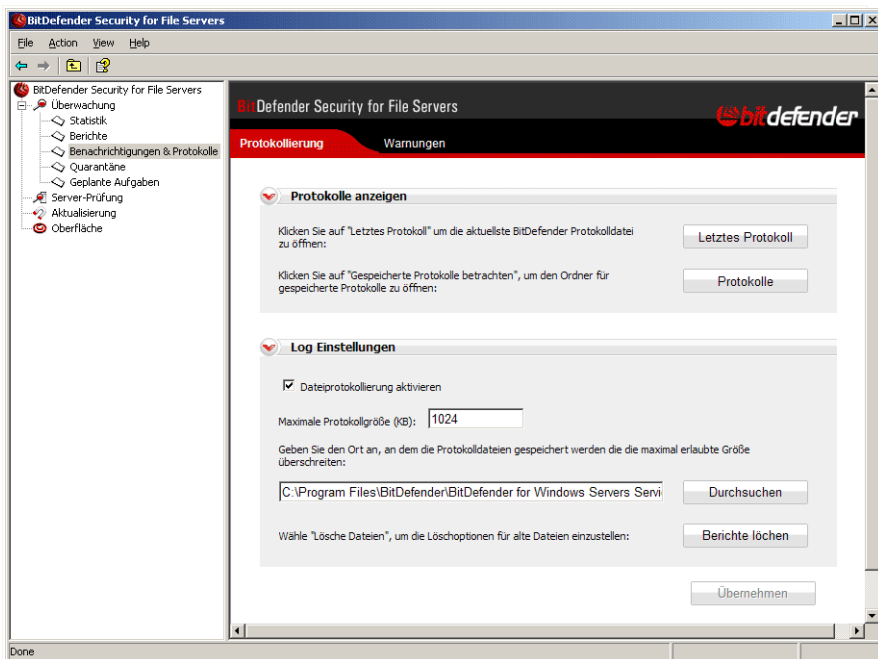
BitDefender ist standardmäßig so konfiguriert, dass die Aktivität protokolliert wird. Das BitDefender Protokoll liefert Ihnen eine umfangreiche Liste der Ereignisse, die während des Produktbetriebs aufgetreten sind.



Beachten Sie

Standardmäßig wird die Berichtsdatei gespeichert unter:
?:\Programme\BitDefender\BitDefender für Windows Servers
Services\BDLog.

Um die Protokollierung zu konfigurieren und Protokolldateien zu betrachten, klicken Sie auf **Benachrichtigungen & Protokolle** im Baummenu (unter **Überwachung**) und dann auf den Tab **Protokollierung**.



Protokolle

Protokolle prüfen

Klicken Sie auf **Letztes Protokoll anzeigen**, um die letzte Protokolldatei zu öffnen.

Wenn Sie ein Größenlimit für die Protokolldatei festgelegt haben, können Sie alle gespeicherten Protokolldateien sehen. Klicken Sie auf **Gespeicherte Protokolle**

anzeigen, wählen Sie dann die Protokolldatei, die Sie betrachten möchten und doppelklicken Sie dann darauf.

Protokollierung konfigurieren

Um die Produktaktivität in einer Datei zu protokollieren, wählen Sie **Dateiprotokollierung aktivieren**.

BitDefender erstellt die Protokolldatei in `?:\Programme\BitDefender\BitDefender für Windows Servers Services\BDLog`. Wenn die Datei die Größe von 1024 KB erreicht, wird standardmäßig eine neue Protokolldatei erstellt.

Legen Sie das Größenlimit der Protokolldateien in dem Feld **Maximale Größe von Protokolldateien** fest. Wenn Sie keine Beschränkung möchten, geben Sie 0 in das Feld ein.

Sie können einen Ordner angeben, in dem Dateien, die das festgelegte Größenlimit überschreiten, gespeichert werden. Geben Sie seinen Pfad entweder in das entsprechende Feld ein oder klicken Sie auf **Durchsuchen**, suchen Sie den Ordner und klicken Sie dann auf **OK** um den Speicherort festzulegen.

Um den Zeitraum einzustellen, für den Berichte gespeichert werden, klicken Sie **Berichte Löschen**. Geben Sie die Anzahl der Stunden / Tage / Wochen / Monate für die Aufbewahrung ein und klicken Sie auf **OK**.

Klicken Sie auf **Anwenden**, um die Änderungen zu speichern.

8.5. Quarantäne

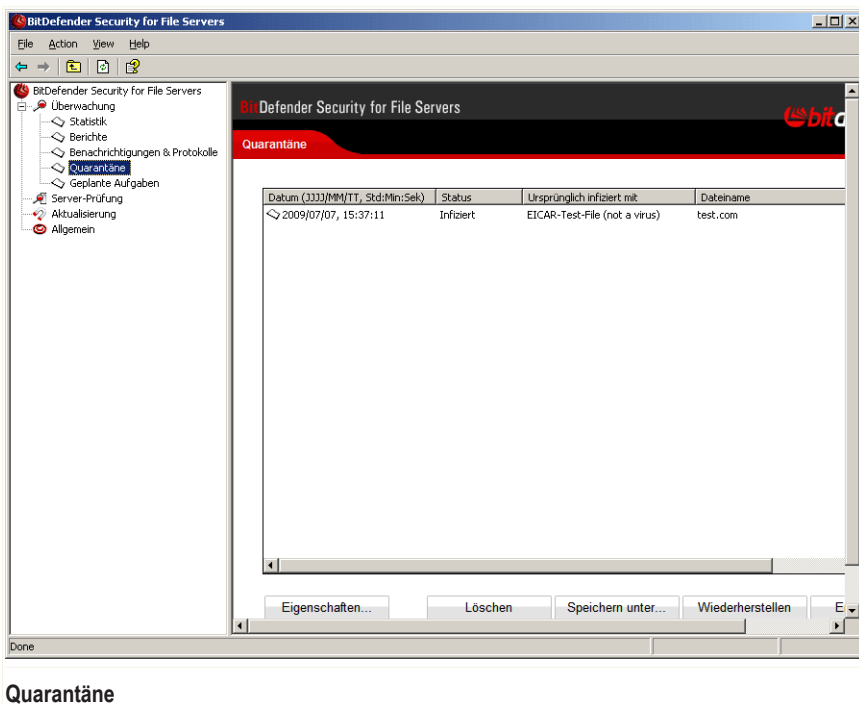
Mit BitDefender können infizierte oder verdächtige Dateien in einem sicheren Bereich, der Quarantäne, isoliert werden. Indem diese Dateien isoliert werden, kann durch sie keine Infektion ausgelöst werden.



Wichtig

Der Quarantäne-Ordner ist für die Prüfungen On-Access und On-Demand identisch.

Um die Dateien in der Quarantäne zu sehen und sie zu verwalten, klicken Sie bitte auf **Quarantäne** im Baummenu (unter **Überwachung**).



Sie können eine Liste der Dateien in der Quarantäne in der Tabelle aufgelistet sehen. Für jede Datei in der Quarantäne werden folgende Informationen angegeben: Das Datum und die Uhrzeit wann sie in die Quarantäne verschoben wurde, der Status (infiziert/verdächtig), der Virennamen, der Ursprungsort und der Dateiname.

Dateien in der Quarantäne sind verschlüsselt. Um eine Datei in der Quarantäne zu öffnen oder auszuführen wählen Sie sie aus und klicken Sie dann auf **Auf Festplatte speichern** um die Datei zu entschlüsseln.

8.5.1. Die Quarantäne verwalten

Verwenden Sie die zur Verfügung stehenden Schaltflächen um die Dateien in der Quarantäne zu verwalten:

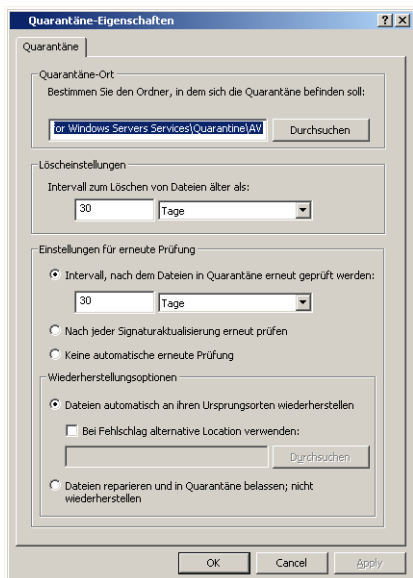
- **Löschen** - löscht eine oder mehrere ausgewählte Dateien.
- **Speichern unter** - entschlüsselt die gewählten Dateien in der Quarantäne und speichert sie auf der Festplatte. Auf diese Weise können Sie diese Dateien öffnen oder ausführen.
- **Wiederherstellen** - entschlüsselt gewählte Dateien in der Quarantäne und stellt sie an ihrem ursprünglichen Ort wieder her.
- **Erneut prüfen** - prüft ausgewählte Dateien in der Quarantäne erneut.

Durch eine erneute Prüfung schon länger in der Quarantäne befindlicher Dateien mit den neuesten Malware-Signaturen können diese Dateien eventuell repariert und an ihrem ursprünglichen Ort wiederhergestellt werden.

- **Eigenschaften** - öffnet ein Fenster, in dem Sie **Quarantäne-Einstellungen** vornehmen können.

Quarantäne-Einstellungen konfigurieren

Wenn Sie die Quarantäne-Einstellungen konfigurieren möchten, klicken Sie auf **Eigenschaften**.



Quarantäne-Eigenschaften

Die folgenden Einstellungen können konfiguriert werden.

● Quarantäne-Ort

Sie können den Ordner, in dem sich die Quarantäne befindet ändern. Geben Sie den Pfad zu dem neuen Ordner in das Editierfeld ein oder klicken Sie auf die Schaltfläche **Durchsuchen** um einen neuen Speicherplatz festzulegen. Der Standard Ort der Quarantäne Dateien ist: C:\Programme\BitDefender\BitDefender for Windows Servers Services\Quarantine.

● Löscheinstellungen

Standardmäßig werden Dateien in der Quarantäne, die älter als 30 Tage sind, automatisch gelöscht. Um den Zeitraum der Speicherung der Dateien in der Quarantäne zu festzulegen, geben Sie die Anzahl der Stunden/Tage/Wochen/Monate in das entsprechende Feld ein.

● Einstellungen für erneute Prüfung

BitDefender prüft automatisch alle Dateien in der Quarantäne alle 30 Tage erneut. Sie können dieses Intervall ändern und eine beliebige Anzahl an Stunden/Tagen/Wochen/Monaten einstellen; alternativ können erneute Prüfungen nach jeder Malware-Signaturaktualisierung ausgeführt werden. Die Fusion kann auch völlig deaktiviert werden.



Beachten Sie

Es wird empfohlen, Objekte in der Quarantäne nach jeder Malware-Signaturaktualisierung erneut zu prüfen.

● Wiederherstellungsoptionen

Standardmäßig werden reparierte Objekte automatisch an ihrem ursprünglichen Ort wiederhergestellt.

Die Wiederherstellung kann in einigen Fällen fehlschlagen (wenn z. B. der ursprüngliche Ort nicht mehr existiert). Deshalb können Sie einen alternativen Ort einstellen, indem Sie das entsprechende Kästchen markieren und einen neuen Ort eingeben.

Um die Wiederherstellung reparierter Dateien zu deaktivieren, wählen Sie **Dateien reparieren und in Quarantäne belassen**.

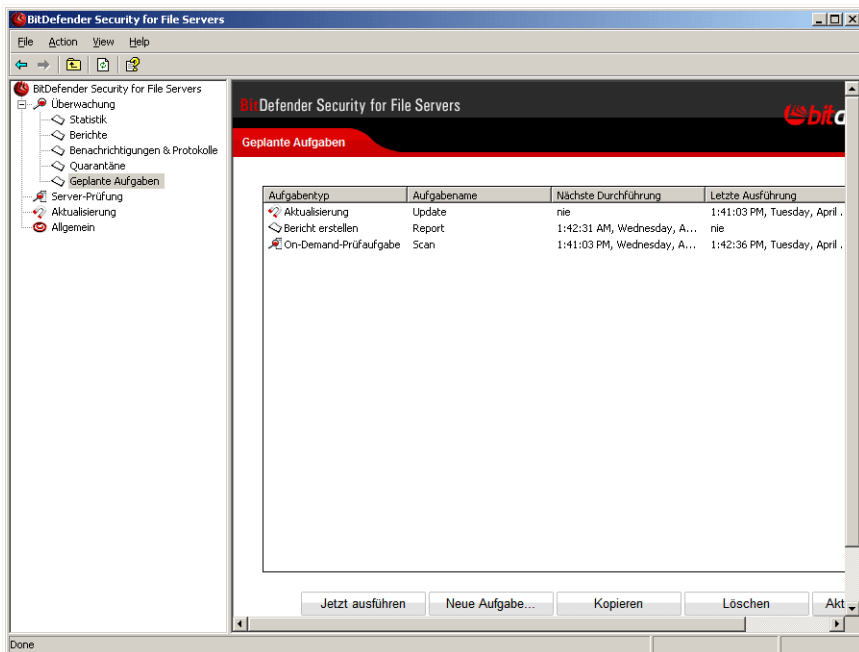
Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.

8.6. Geplante Aufgaben

Zeitgesteuerte Aufgaben bieten eine weitreichende Flexibilität und helfen Ihnen dabei, administrative Sicherheitsaufgaben durchzuführen, ohne dass dabei die Leistung Ihres Servers beeinträchtigt wird. Sie können BitDefender so einstellen, dass bestimmte Aufgaben nur ein Mal oder regelmäßig ausgeführt werden. Folgende Aufgaben können eingeplant werden:

- On-Demand Prüfvorgänge.
- Update-Prozesse.
- Aufgaben zur Erstellung eines Berichts.

Klicken Sie auf **Zeitgesteuerte Aufgaben** im Baummenu (unter **Überwachung**) um zeitgesteuerte Aufgaben zu erstellen/konfigurieren.



Geplante Aufgaben

Sie können alle eingeplanten Aufgaben aufgelistet in der Tabelle sehen. Für jede Aufgabe werden folgende Informationen zur Verfügung gestellt: Der Name der Aufgabe, der Zeitpunkt der letzten Durchführung, der Zeitpunkt der nächsten eingestellten Durchführung und der Status.

8.6.1. Geplante Aufgaben verwalten

Um geplante Aufgaben zu verwalten, verwenden Sie diese Schaltflächen:

- **Jetzt durchführen** - führt eine ausgewählte zeitgesteuerte Aufgabe durch.
- **Neue Aufgabe** - startet den Assistenten, der Ihnen beim Erstellen einer neuen zeitgesteuerten Aufgabe hilft.



Beachten Sie

Der Konfigurations-Assistent unterscheidet sich für jede zeitgesteuerte Aufgabe.

- **Kopieren** - kopiert eine oder mehrere ausgewählte Aufgaben.
- **Löschen** - löscht eine oder mehrere ausgewählte Aufgaben. Sie werden aufgefordert, Ihre Auswahl zu bestätigen. Klicken Sie dazu auf **Ja**.
- **Aktivieren/Deaktivieren** - aktiviert/deaktiviert eine oder mehrere ausgewählte Aufgaben.
- **Eigenschaften** - öffnet ein Konfigurationsfenster der ausgewählten Aufgabe, in dem Sie weitere Einstellungen verändern und konfigurieren können.

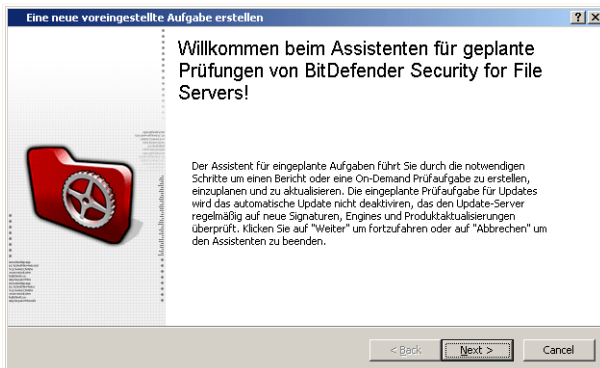
8.6.2. On-Demand Prüfaufgaben

Aufgaben zeitlich einplanen

Sie erstellen eine neue zeitgesteuerte Aufgabe, indem Sie auf **Neue Aufgabe** klicken. Es erscheint ein Konfigurationsassistent, der Sie durch den Prozess der Erstellung einer zeitgesteuerten Aufgabe begleitet.

Befolgen Sie diese Schritte um eine zeitgesteuerte On-Demand Prüfaufgabe einzustellen:

Schritt 1/7 - Willkommen zum Assistenten für zeitgesteuerte Aufgaben



Willkommen

Klicken Sie auf **Weiter**.

Schritt 2/7 – Aufgabentyp wählen

Eine neue voreingestellte Aufgabe erstellen

Auswählen des Aufgabentyps

Aufgabe:
On-Demand

Aufgabentyp:

☐ Update-Aufgabe

☐ Aufgabe zur Berichterstellung

☒ On-Demand-Prüfaufgabe

< Back Next > Cancel

Auswählen des Aufgabentyps

Bitte geben Sie den Namen der Aufgabe an und wählen Sie **On-Demand Prüfaufgabe**.
Klicken Sie auf **Weiter**.

Schritt 3/7 – Zeitsteuerung konfigurieren

Eine neue voreingestellte Aufgabe erstellen

Konfigurieren Sie die Planungseinstellungen

Ausführung der Aufgabe einstellen:
periodisch

Startdatum: 4/12/2011

Enddatum: 4/12/2011

Startzeit: 1:41:03 PM alle: 1 Tage

< Back Next > Cancel

Konfigurieren Sie den Aufgabenplan.

Geben Sie den Zeitplan für die Aufgabe an.
Sie müssen eine der folgenden Optionen aus dem Menu wählen:

- **Einmal** - führt das Update nur einmal, zu einem bestimmten Zeitpunkt aus.

Geben Sie den Zeitpunkt des Starts und des Endes in die Felder **Startdatum/Ende** ein.

- **Periodisch** - führt die Aufgabe periodisch, in bestimmten zeitlichen Abständen (Minuten, Stunden, Tage, Wochen, Monate, Jahre) aus. Der Startpunkt wird mit Datum und Uhrzeit festgelegt.

Um die nötigen Einstellungen zu konfigurieren, befolgen Sie die folgenden Schritte:

1. Geben Sie das Startdatum in das Feld **Startdatum** ein.
2. Wenn Sie möchten, dass die Aufgabe mehrmals bis zu einem bestimmten Datum ausgeführt wird, markieren Sie **Ende** und geben Sie das Datum des Endes in das entsprechende Feld ein.
3. Geben Sie die Startzeit in das Feld **Startzeit** ein.
4. Legen Sie die Häufigkeit der Aufgabe fest, indem Sie in das entsprechende Feld die Anzahl der Minuten / Stunden / Tage / Wochen / Monate / Jahre angeben, die zwischen zwei Aufgaben liegen sollen.

- **Wochentage** - um die Aufgabe mehrmals an bestimmten Wochentagen auszuführen, wobei an einem festgelegten Datum/Uhrzeit begonnen wird.

Um die nötigen Einstellungen zu konfigurieren, befolgen Sie die folgenden Schritte:

1. Geben Sie das Startdatum in das Feld **Startdatum** ein.
2. Wenn Sie möchten, dass die Aufgabe mehrmals bis zu einem bestimmten Datum ausgeführt wird, wählen Sie **Ende** und geben Sie das Enddatum in das entsprechende Feld ein.
3. Geben Sie die Startzeit in das Feld **Startzeit** ein.
4. Wählen Sie den Tag oder die Tage an dem/denen die Aufgabe ausgeführt werden soll.

Klicken Sie auf **Weiter**.

Schritt 4/7 - Wählen Sie den Prüfmodus



Wählen Sie den Prüfmodus

Sie können folgende Prüfmodi wählen:

Prüfmodus	Beschreibung
Schnelle Systemprüfung	Hier können die Ordner <i>Programmdateien</i> und <i>Windows</i> mithilfe einer festgelegten Konfiguration der Prüfeinstellungen schnell geprüft werden. Bitte beachten sie, dass nur Anwendungsdateien gespeichert werden, die eine Größe von 10 MB nicht überschreiten.
Tiefgehende Systemprüfung	Bietet eine umfangreiche Prüfung des gesamten File Servers. Durch die voreingestellten Prüfeinstellungen wird die höchste Effizienz bei der Virentdeckung gewährleistet.
Prüfung anpassen	Bietet die Möglichkeit bestimmte Ordner auf dem File Server zu prüfen, indem eine benutzerdefinierte Konfiguration der Prüfeinstellungen angewendet wird.



Wichtig

Um die verfügbaren Einstellungen für den ausgewählten Prüfmodus zu konfigurieren, öffnen Sie das Fenster für die Aufgabenkonfiguration und gehen Sie zu:

- Der Tab **Prüfeinstellungen** um das Prüfziel und die Prüfeinstellungen zu konfigurieren, wenn Sie eine benutzerdefinierte Prüfung ausgewählt haben.
- Der Tab **Aktionen** um die Aktionen festzulegen, die bei entdeckten Dateien durchgeführt werden.
- Der Tab **Benachrichtigungen** um die Benachrichtigungsoptionen zu konfigurieren.

Weitere Informationen finden Sie hier: „*Eigenschaften konfigurieren*“ (S. 71).

Klicken Sie auf **Weiter**.

Schritt 5/7 - Aktionen einstellen



Aktionen einstellen

Sie können verschiedene Aktionen für jede Art der entdeckten Datei auswählen: infiziert, verdächtig oder Rootkit. Wählen Sie die durchzuführende Aktion für die erkannten Dateien aus den entsprechenden Menüs.



Beachten Sie

Sie können zwei Aktionen für Dateien konfigurieren, die infiziert oder verdächtig sind. Die zweite Aktion wird durchgeführt falls die Erste fehlschlägt.

Aktionen für infizierte Dateien. Folgende Aktionen stehen für infizierte Dateien zur Verfügung:

Aktion	Beschreibung
Desinfizieren	Den Malware-Code aus den entdeckten infizierten Dateien entfernen. Die Wiederherstellung kann in einigen Fällen fehlschlagen (wenn die Datei z. B. innerhalb eines bestimmten Archivs ist oder sie von einem laufenden Prozess verwendet wird).
In Quarantäne verschieben	Infizierte Dateien von Ihrer ursprünglichen Position in den Quarantäne-Ordner verschieben. Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht kein Infektionsrisiko?
Löschen	Infizierte Dateien direkt und ohne Warnung von der Festplatte entfernen.
Ignorieren	Nur die entdeckten infizierten Dateien im Prüfbericht protokollieren. Um den Prüfbericht zu sehen, klicken Sie auf Berichte im Baummenu wenn die Prüfung beendet wurde.

Aktionen für verdächtige Dateien. Folgende Aktionen stehen für verdächtige Dateien zur Verfügung:

Aktion	Beschreibung
In Quarantäne verschieben	Infizierte Dateien von Ihrer ursprünglichen Position in den Quarantäne-Ordner verschieben. Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht kein Infektionsrisiko?
Löschen	Verdächtige Dateien direkt und ohne Warnung von der Festplatte entfernen.
Ignorieren	Nur die entdeckten verdächtigen Dateien im Prüfbericht protokollieren. Um den Prüfbericht zu sehen, klicken Sie auf Berichte im Baummene wenn die Prüfung beendet wurde.

Aktionen für Rootkits (verborgene Objekte). Folgende Aktionen stehen für Rootkits zur Verfügung:

Aktion	Beschreibung
Desinfizieren	Den Malware-Kode aus den entdeckten infizierten Dateien entfernen. Die Wiederherstellung kann in einigen Fällen fehlschlagen (wenn die Datei z. B. innerhalb eines bestimmten Archivs ist oder sie von einem laufenden Prozess verwendet wird).
Ignorieren	Nur die entdeckten Rootkits im Prüfbericht protokollieren. Um den Prüfbericht zu sehen, klicken Sie auf Berichte im Baummene wenn die Prüfung beendet wurde.

Klicken Sie auf **Weiter**.

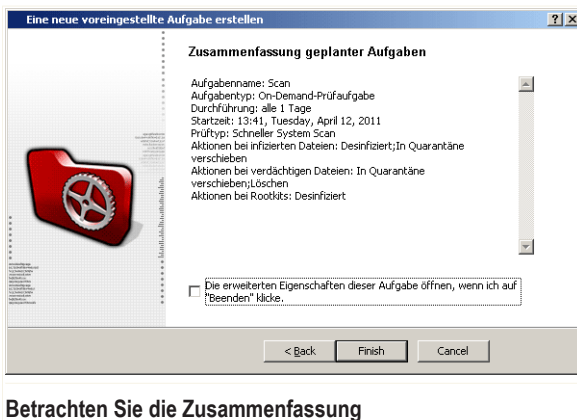
Schritt 6/7 – Benachrichtigungsoptionen konfigurieren



Wählen Sie **Start/Ende der On-Demand Prüfung protokollieren**, um den Start und das Ende der Prüfung in der Bitdefender Protokolldatei aufzuzeichnen. Wenn Sie möchten, dass BitDefender Mail- oder Net Send Benachrichtigungen zu bestimmten Personen sendet, öffnen Sie **Benachrichtigungen & Protokolle**, den Tab **Benachrichtigungen** und konfigurieren Sie das Ereignis **On-Demand Prüfung entsprechend**. Weitere Informationen finden Sie hier: *„Ereignisbenachrichtigung konfigurieren“ (S. 53)*.

Klicken Sie auf **Weiter**.

Schritt 7/7 – Zusammenfassung betrachten



In diesem Fenster können Sie die Aufgabeneinstellungen überprüfen. Sie können Änderungen vornehmen, indem Sie zu den vorherigen Schritten zurückkehren (klicken Sie auf **Zurück**).

Wählen Sie **Erweiterte Eigenschaften dieser Aufgabe öffnen**, wenn ich auf **"Beenden"** klicke wenn Sie möchten, dass das Fenster **Eigenschaften** dieser Aufgabe geöffnet wird, wenn Sie den Assistenten beenden. In diesem Fenster können Sie die weitere Einstellungen konfigurieren und die Aufgabe bearbeiten. Weitere Informationen finden Sie hier: „*Eigenschaften konfigurieren*“ (S. 71).

Klicken Sie auf **Beenden**, um die zeitgesteuerte Aufgabe zu speichern.

**Beachten Sie**

Die neue Aufgabe wird nun im Abschnitt **Zeitgesteuerte Aufgaben** angezeigt.

Eigenschaften konfigurieren

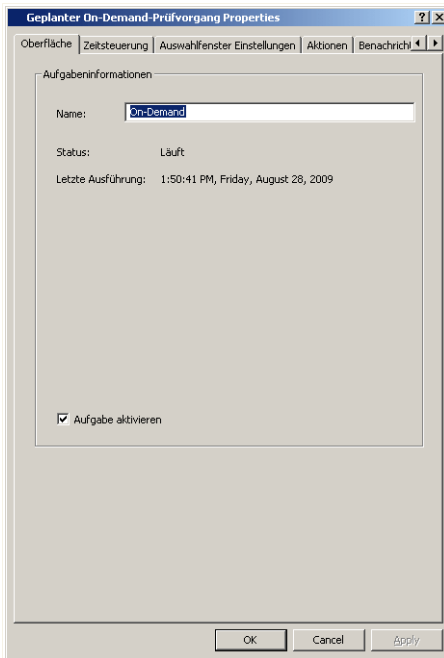
Um eine vorhandene zeitgesteuerte Aufgabe zu bearbeiten oder um weitere Einstellungen zu konfigurieren, die nicht im Konfigurationsassistenten zur Verfügung stehen, doppelklicken Sie einfach auf die Aufgabe oder wählen Sie sie aus und klicken Sie auf **Eigenschaften**. Das Konfigurationsfenster wird erscheinen.

**Beachten Sie**

Um das Konfigurationsfenster zu öffnen, können Sie auch **Erweiterte Eigenschaften öffnen**, wenn ich auf **"Beenden"** klicke im letzten Schritt des Assistenten wählen.

Allgemeine Informationen betrachten

Öffnen Sie das Konfigurationsfenster, um allgemeine Informationen zu betrachten.



Allgemein

Hier finden Sie allgemeine Informationen über die Aufgabe (Name, Status und der letzte Zeitpunkt der Ausführung). Wenn Sie den Namen der Aufgabe ändern möchten, geben Sie einen neuen Namen in das entsprechende Feld ein.

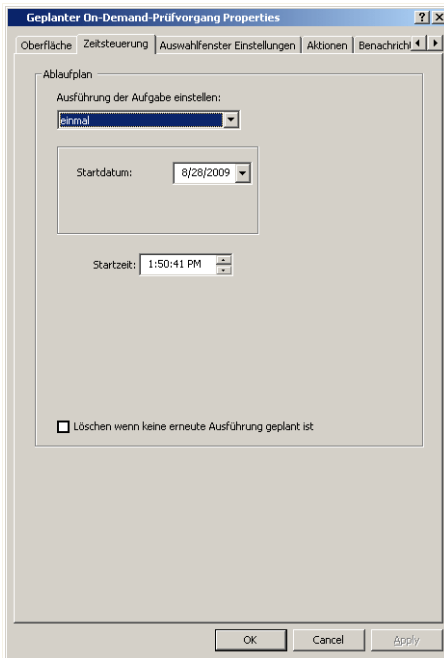
Um die Aufgabe zu aktivieren, wählen Sie **Aufgabe aktivieren**. Lassen Sie das Kontrollkästchen andererseits frei.

Klicken Sie auf **Anwenden**, um die Änderungen zu speichern. Wenn Sie die Änderungen speichern und das Konfigurationsfenster schließen möchten, klicken Sie auf **OK**.

Wenn das Konfigurationsfenster schließen möchten ohne die Änderungen zu speichern, klicken Sie auf **Abbrechen**.

Zeitsteuerung bearbeiten

Klicken Sie auf den Tab **Zeitsteuerung** im Konfigurationsfenster um die Zeitsteuerung zu bearbeiten.



Plan

Geben Sie den Zeitplan für die Aufgabe an.

Sie müssen eine der folgenden Optionen aus dem Menu wählen:

- **Einmal** - führt das Update nur einmal, zu einem bestimmten Zeitpunkt aus.

Geben Sie den Zeitpunkt des Starts und des Endes in die Felder **Startdatum/Ende** ein.

- **Periodisch** - führt die Aufgabe periodisch, in bestimmten zeitlichen Abständen (Minuten, Stunden, Tage, Wochen, Monate, Jahre) aus. Der Startpunkt wird mit Datum und Uhrzeit festgelegt.

Um die nötigen Einstellungen zu konfigurieren, befolgen Sie die folgenden Schritte:

1. Geben Sie das Startdatum in das Feld **Startdatum** ein.
2. Wenn Sie möchten, dass die Aufgabe mehrmals bis zu einem bestimmten Datum ausgeführt wird, markieren Sie **Ende** und geben Sie das Datum des Endes in das entsprechende Feld ein.
3. Geben Sie die Startzeit in das Feld **Startzeit** ein.
4. Legen Sie die Häufigkeit der Aufgabe fest, indem Sie in das entsprechende Feld die Anzahl der Minuten / Stunden / Tage / Wochen / Monate / Jahre angeben, die zwischen zwei Aufgaben liegen sollen.

- **Wochentage** - um die Aufgabe mehrmals an bestimmten Wochentagen auszuführen, wobei an einem festgelegten Datum/Uhrzeit begonnen wird.

Um die nötigen Einstellungen zu konfigurieren, befolgen Sie die folgenden Schritte:

1. Geben Sie das Startdatum in das Feld **Startdatum** ein.
2. Wenn Sie möchten, dass die Aufgabe mehrmals bis zu einem bestimmten Datum ausgeführt wird, wählen Sie **Ende** und geben Sie das Enddatum in das entsprechende Feld ein.
3. Geben Sie die Startzeit in das Feld **Startzeit** ein.
4. Wählen Sie den Tag oder die Tage an dem/denen die Aufgabe ausgeführt werden soll.

Wählen Sie **Löschen wenn keine erneute Ausführung geplant ist** - löscht die Aufgabe nach der letzten Ausführung.

Klicken Sie auf **Anwenden**, um die Änderungen zu speichern. Wenn Sie die Änderungen speichern und das Konfigurationsfenster schließen möchten, klicken Sie auf **OK**.

Wenn das Konfigurationsfenster schließen möchten ohne die Änderungen zu speichern, klicken Sie auf **Abbrechen**.

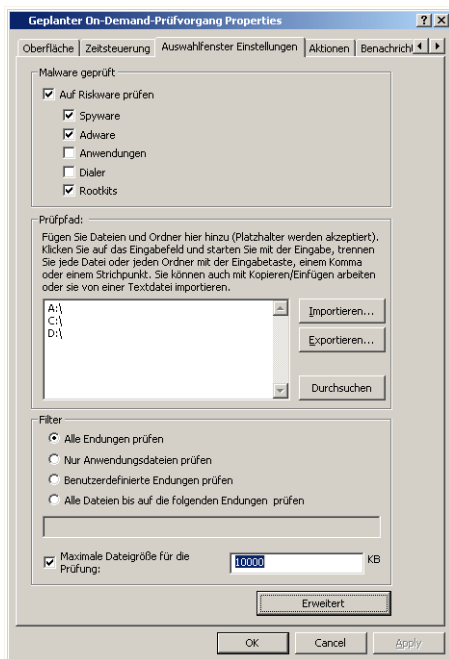
Einstellungen konfigurieren

Klicken Sie auf den Tab **Prüfeinstellungen** im Konfigurationsfenster, um das Prüfziel und die Prüfeinstellungen zu konfigurieren.



Beachten Sie

Wenn Sie eine schnelle oder tiefe Systemprüfung voreingestellt haben, können Sie nur das festgelegte Prüfziel und die Prüfeinstellungen sehen.



Einstellungen

Spezielle Malware von der Prüfung ausschließen

Sie können BitDefender so einstellen, dass neben den Virensignaturen auch die Signaturen folgender Bedrohungen verwendet werden:

- Spyware
- Adware
- Anwendungen
- Dialers
- Rootkits

Lassen sie zu diesem Zweck die Kontrollkästchen zu **Auf Riskware prüfen** und zu den spezifischen Malware-Bedrohungen, auf die geprüft werden soll, markiert.



Wichtig

Alle erkannte Malware wird als infiziert behandelt.

Wenn Sie möchten, dass BitDefender nur Virensignaturen für die Prüfung auf Basis von Signaturen verwendet, so lassen Sie das Kontrollkästchen zu **Auf Riskware prüfen** frei.

Festlegen der Zielobjekte

Befolgen Sie eine der folgenden Möglichkeiten, um spezielle Objekte (Laufwerke, Dateien, Ordner) festzulegen, die geprüft werden sollen:

- Geben Sie in das Editierfeld den vollständigen Pfad der zu prüfenden Objekte ein, wobei Sie diese mit der Eingabetaste, einem Komma oder Strichpunkt trennen müssen.
- Klicken Sie auf **Durchsuchen** und wählen Sie die zu prüfenden Objekte.
- Wenn Sie über eine Textdatei verfügen, die eine Liste der Locations (von Dateien und Ordnern) enthält, die geprüft werden sollen, klicken Sie auf **Importieren** und laden Sie die entsprechende Datei. Sie können die Locations auch aus der Textdatei kopieren und direkt in das Editierfeld einfügen.

Um die Liste der Dateien und Ordner als eine Textdatei zu speichern, klicken Sie auf **Exportieren**.

Dateien anhand der Endungen prüfen

Bestimmte Dateisorten sind anfälliger auf Viren als andere. So ist zum Beispiel das Risiko beim Ausführen einer `.exe` Datei höher, als beim Öffnen einer `.txt` oder einer `.gif` Datei.

Um festzulegen welche Dateisorten geprüft werden sollen, wählen Sie zwischen den folgenden Optionen wählen:

Optionen	Beschreibung
Alle Endungen prüfen	Prüft alle vorhandenen Dateien.
Nur Anwendungsdateien prüfen	Nur Anwendungsdateien werden geprüft. Diese Kategorie ist auf Dateien mit den folgenden Erweiterungen beschränkt: 386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst;

Optionen	Beschreibung
	pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xism; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp Viren werden normalerweise über Anwendungsdateien übertragen. Deshalb sollten diese Dateien immer überprüft werden.
Benutzerdefinierte Endungen prüfen	Nur Dateien mit den festgelegten Endungen werden geprüft. Sie müssen in das Editierfeld die Dateieendungen eingeben, die von BitDefender geprüft werden sollen, wobei diese mit Strichpunkten (",") zu trennen sind.
Alle bis auf die folgenden Endungen prüfen	Die Dateien mit den festgelegten Endungen werden NICHT geprüft. Sie müssen in das Editierfeld die Dateieendungen eingeben, die NICHT von BitDefender geprüft werden sollen, wobei diese mit Strichpunkten (",") zu trennen sind. Sie sollten Dateiearten, die bekannt für Vren sind nicht von der Prüfung ausschließen, wie beispielsweise .exe, .doc, .ppt, .xls, .rtf, .pif, .bat und Andere.

Dateien anhand der Größe prüfen.

Die Prüfung großer Dateien erfordert zusätzliche Systemressourcen, was das System verlangsamt.

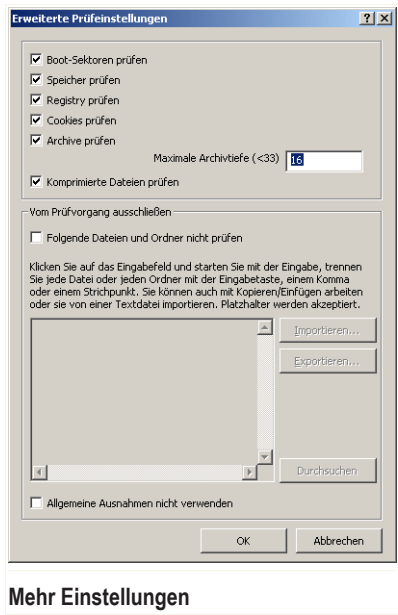
Legen Sie das Größenlimit (in KB) der zu prüfenden Dateien in dem Feld **Maximale Größe von zu prüfenden Dateien** fest. Wenn Sie beispielsweise 2000 eingeben, werden alle Dateien die größer als 2000 KB sind von der Prüfung ausgeschlossen.

Wenn Sie möchten, das alle Dateien, unabhängig von deren Größe geprüft werden, befolgen Sie eine der folgenden Möglichkeiten:

- Lassen Sie das Kontrollkästchen zu **Maximale Größe von zu prüfenden Dateien** frei.
- Geben Sie als Größenbegrenzung 0 KB ein.

Weitere Einstellungen und Ausnahmen konfigurieren

Um weitere Einstellungen oder Ausnahmen der On-Demand Prüfung vorzunehmen, klicken Sie auf **Erweitert**. Ein neues Konfigurationsfenster wird sich öffnen.



Mehr Einstellungen

Folgende erweiterte Prüfeinstellungen können konfiguriert werden:

Optionen	Beschreibung
Boot-Sektoren	Den Bootsektor der verfügbaren Laufwerke prüfen.
Speicher prüfen	Den Systemspeicher prüfen.
Registry prüfen	Die Windows-Registry prüfen.
Cookies prüfen	Cookie-Dateien prüfen.
Archive prüfen	Archivierte Dateien prüfen. Sie können eine maximale Archivtiefe festlegen, um Dateien zu prüfen, die mehrfach archiviert wurden. Wenn Sie Dateien prüfen wollen, egal wie häufig diese archiviert wurden, stellen Sie die maximale Archivtiefe auf 0 ein. Wenn Sie diese Option wählen, wird die Leistung des Systems verlangsamt und die Prüfzeit verlängert.
Komprimierte Dateien prüfen	Komprimierte Dateien prüfen.

Um Dateien und Ordner von der On-Demand-Prüfung auszuschließen:

1. Wählen Sie **Folgende Dateien und Ordner nicht prüfen**.
2. Wählen Sie eine der folgenden Methoden:

- Geben Sie in das Editierfeld den vollständigen Pfad der Dateien und Ordner ein, die nicht geprüft werden sollen, wobei Sie diese mit der Eingabetaste, einem Komma oder Strichpunkt trennen müssen.
- Klicken Sie auf **Durchsuchen** und wählen Sie die Dateien und Ordner, die nicht geprüft werden sollen.
- Wenn Sie über eine Textdatei verfügen, die eine Liste der Locations (von Dateien und Ordnern) enthält, die nicht geprüft werden sollen, klicken Sie auf **Importieren** und laden Sie die entsprechende Datei. Sie können die Locations auch aus der Textdatei kopieren und direkt in das Editierfeld einfügen.

Um die Liste der Dateien und Ordner als eine Textdatei zu speichern, klicken Sie auf **Exportieren**. Auf diese Weise können Sie diese Liste auf andere File Server laden, um die Prüfausnahmen zu konfigurieren.

Klicken Sie auf **Anwenden**, um die Änderungen zu speichern. Wenn Sie die Änderungen speichern und das Konfigurationsfenster schließen möchten, klicken Sie auf **OK**.

Wenn das Konfigurationsfenster schließen möchten ohne die Änderungen zu speichern, klicken Sie auf **Abbrechen**.

Konfigurieren der Aktionen

Klicken Sie auf den Tab **Aktionen** im Konfigurationsfenster, um die Aktionen zu konfigurieren, die bei infizierten Dateien durchgeführt werden sollen.

Geplanter On-Demand-Prüfvorgang

Allgemein

Plan

Auswählen der Einstellungen

Aktionen

Benachrichtigungen

Infizierte Dateien

Aktion, die für infizierte Dateien angewendet wird:

Direktverbindung

Desinfiziert

Aktionsoptionen

In Quarantäne verschieben

Verdächtige Dateien

Aktion, die für verdächtige Dateien angewendet wird:

Direktverbindung

In Quarantäne verschieben

Aktionsoptionen

Löschen

Rootkits

Wählen Sie die Aktion, die durchgeführt werden soll, wenn Rootkits gefunden werden:

Desinfiziert

OK

Cancel

Apply

Aktionen

Sie können verschiedene Aktionen für jede Art der entdeckten Datei auswählen: infiziert, verdächtig oder Rootkit. Wählen Sie die durchzuführende Aktion für die erkannten Dateien aus den entsprechenden Menüs.



Beachten Sie

Sie können zwei Aktionen für Dateien konfigurieren, die infiziert oder verdächtig sind. Die zweite Aktion wird durchgeführt falls die Erste fehlschlägt.

Aktionen für infizierte Dateien. Folgende Aktionen stehen für infizierte Dateien zur Verfügung:

Aktion	Beschreibung
Desinfizieren	Den Malware-Code aus den entdeckten infizierten Dateien entfernen. Die Wiederherstellung kann in einigen Fällen fehlschlagen (wenn die Datei z. B. innerhalb eines bestimmten Archivs ist oder sie von einem laufenden Prozess verwendet wird).
In Quarantäne verschieben	Infizierte Dateien von Ihrer ursprünglichen Position in den Quarantäne-Ordner verschieben. Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht kein Infektionsrisiko?

Aktion	Beschreibung
Löschen	Infizierte Dateien direkt und ohne Warnung von der Festplatte entfernen.
Ignorieren	Nur die entdeckten infizierten Dateien im Prüfbericht protokollieren. Um den Prüfbericht zu sehen, klicken Sie auf Berichte im Baumannu wenn die Prüfung beendet wurde.

Aktionen für verdächtige Dateien. Folgende Aktionen stehen für verdächtige Dateien zur Verfügung:

Aktion	Beschreibung
In Quarantäne verschieben	Infizierte Dateien von Ihrer ursprünglichen Position in den Quarantäne-Ordner verschieben. Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht kein Infektionsrisiko?
Löschen	Verdächtige Dateien direkt und ohne Warnung von der Festplatte entfernen.
Ignorieren	Nur die entdeckten verdächtigen Dateien im Prüfbericht protokollieren. Um den Prüfbericht zu sehen, klicken Sie auf Berichte im Baumannu wenn die Prüfung beendet wurde.

Aktionen für Rootkits (verborgene Objekte). Folgende Aktionen stehen für Rootkits zur Verfügung:

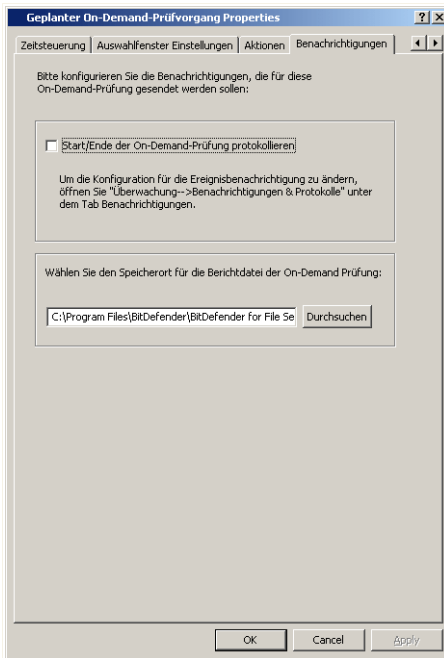
Aktion	Beschreibung
Desinfizieren	Den Malware-Code aus den entdeckten infizierten Dateien entfernen. Die Wiederherstellung kann in einigen Fällen fehlschlagen (wenn die Datei z. B. innerhalb eines bestimmten Archivs ist oder sie von einem laufenden Prozess verwendet wird).
Ignorieren	Nur die entdeckten Rootkits im Prüfbericht protokollieren. Um den Prüfbericht zu sehen, klicken Sie auf Berichte im Baumannu wenn die Prüfung beendet wurde.

Klicken Sie auf **Anwenden**, um die Änderungen zu speichern. Wenn Sie die Änderungen speichern und das Konfigurationsfenster schließen möchten, klicken Sie auf **OK**.

Wenn das Konfigurationsfenster schließen möchten ohne die Änderungen zu speichern, klicken Sie auf **Abbrechen**.

Benachrichtigungen konfigurieren

Klicken sie auf den Tab **Benachrichtigungen** im Konfigurationsfenster, um die Benachrichtigungsoptionen zu konfigurieren.



Benachrichtigungen

Wählen Sie **Start/Ende der On-Demand Prüfung protokollieren**, um den Start und das Ende der Prüfung in der Bitdefender Protokolldatei aufzuzeichnen. Wenn Sie möchten, dass BitDefender Mail- oder Net Send Benachrichtigungen zu bestimmten Personen sendet, öffnen Sie **Benachrichtigungen & Protokolle**, den Tab **Benachrichtigungen** und konfigurieren Sie das Ereignis **On-Demand Prüfung entsprechend**. Weitere Informationen finden Sie hier: „*Ereignisbenachrichtigung konfigurieren*“ (S. 53).

Ein detaillierter Prüfbericht wird jedes Mal erstellt, wenn Sie eine On-Demand-Prüfung durchführen. Der Bericht wird im XML-Format erstellt und kann mithilfe eines Browsers betrachtet werden. Um einen Bericht zu betrachten, öffnen Sie **Berichte**.

Standardmäßig werden die Berichte der On-Demand-Prüfung im Ordner C:\Programmdateien\BitDefender\BitDefender Security for File Server\Berichte gespeichert. Falls Sie einen anderen Speicherort wählen möchten, klicken Sie auf **Durchsuchen** und wählen Sie den Ordner in dem die Berichte gespeichert werden sollen.

Klicken Sie auf **Anwenden**, um die Änderungen zu speichern. Wenn Sie die Änderungen speichern und das Konfigurationsfenster schließen möchten, klicken Sie auf **OK**.

Wenn das Konfigurationsfenster schließen möchten ohne die Änderungen zu speichern, klicken Sie auf **Abbrechen**.

8.6.3. Update-Aufgaben

Aufgaben zeitlich einplanen

Sie erstellen eine neue zeitgesteuerte Aufgabe, indem Sie auf **Neue Aufgabe** klicken. Es erscheint ein Konfigurationsassistent, der Sie durch den Prozess der Erstellung einer zeitgesteuerten Aufgabe begleitet.

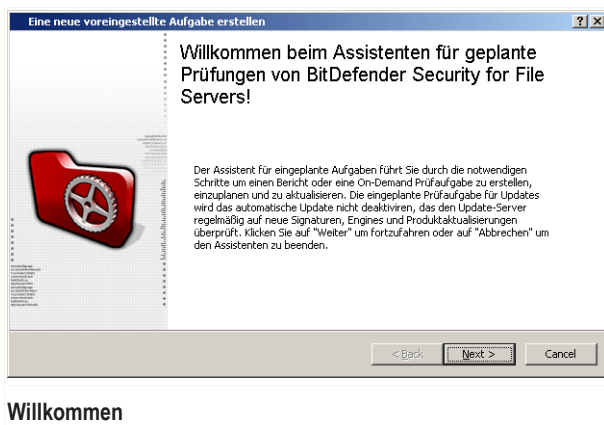


Beachten Sie

Die zeitgesteuerten Update-Aufgaben haben keinen Einfluss auf das automatische Update.

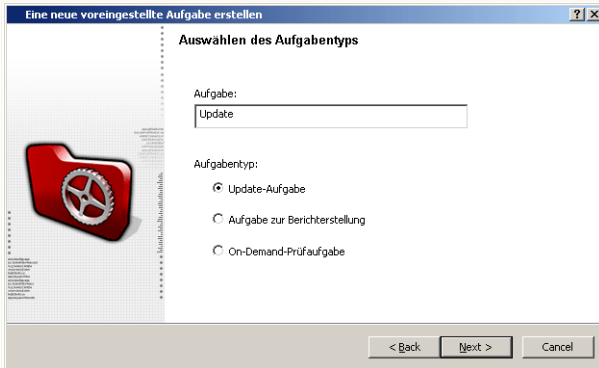
So richten Sie eine zeitgesteuerte Update-Aufgabe ein:

Schritt 1/4 - Willkommen zum Assistenten für zeitgesteuerte Aufgaben



Klicken Sie auf **Weiter**.

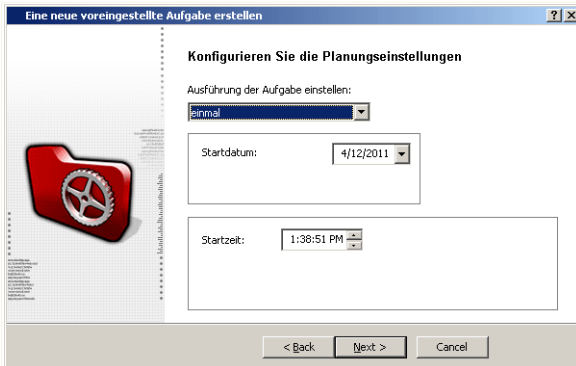
Schritt 2/4 – Aufgabentyp wählen



Auswählen des Aufgabentyps

Bitte geben Sie den Namen der Aufgabe an und wählen Sie **Update-Aufgabe**.
Klicken Sie auf **Weiter**.

Schritt 3/4 – Zeitsteuerung konfigurieren



Konfigurieren Sie den Aufgabenplan.

Geben Sie den Zeitplan für die Aufgabe an.
Sie müssen eine der folgenden Optionen aus dem Menu wählen:

- **Einmal** - führt das Update nur einmal, zu einem bestimmten Zeitpunkt aus.

Geben Sie den Zeitpunkt des Starts und des Endes in die Felder **Startdatum/Ende** ein.

- **Periodisch** - führt die Aufgabe periodisch, in bestimmten zeitlichen Abständen (Minuten, Stunden, Tage, Wochen, Monate, Jahre) aus. Der Startpunkt wird mit Datum und Uhrzeit festgelegt.

Um die nötigen Einstellungen zu konfigurieren, befolgen Sie die folgenden Schritte:

1. Geben Sie das Startdatum in das Feld **Startdatum** ein.
2. Wenn Sie möchten, dass die Aufgabe mehrmals bis zu einem bestimmten Datum ausgeführt wird, markieren Sie **Ende** und geben Sie das Datum des Endes in das entsprechende Feld ein.
3. Geben Sie die Startzeit in das Feld **Startzeit** ein.
4. Legen Sie die Häufigkeit der Aufgabe fest, indem Sie in das entsprechende Feld die Anzahl der Minuten / Stunden / Tage / Wochen / Monate / Jahre angeben, die zwischen zwei Aufgaben liegen sollen.

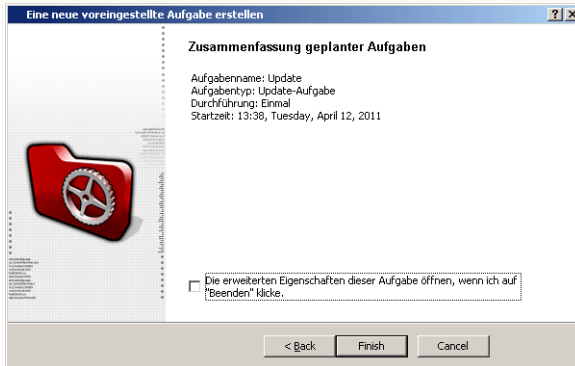
- **Wochentage** - um die Aufgabe mehrmals an bestimmten Wochentagen auszuführen, wobei an einem festgelegten Datum/Uhrzeit begonnen wird.

Um die nötigen Einstellungen zu konfigurieren, befolgen Sie die folgenden Schritte:

1. Geben Sie das Startdatum in das Feld **Startdatum** ein.
2. Wenn Sie möchten, dass die Aufgabe mehrmals bis zu einem bestimmten Datum ausgeführt wird, wählen Sie **Ende** und geben Sie das Enddatum in das entsprechende Feld ein.
3. Geben Sie die Startzeit in das Feld **Startzeit** ein.
4. Wählen Sie den Tag oder die Tage an dem/denen die Aufgabe ausgeführt werden soll.

Klicken Sie auf **Weiter**.

Schritt 4/4 – Zusammenfassung



Betrachten Sie die Zusammenfassung

In diesem Fenster können Sie die Aufgabeneinstellungen überprüfen. Sie können Änderungen vornehmen, indem Sie zu den vorherigen Schritten zurückkehren (klicken Sie auf **Zurück**).

Wählen Sie **Erweiterte Eigenschaften dieser Aufgabe öffnen, wenn ich auf "Beenden" klicke** wenn Sie möchten, dass das Fenster **Eigenschaften** dieser Aufgabe geöffnet wird, wenn Sie den Assistenten beenden. In diesem Fenster können Sie die weitere Einstellungen konfigurieren und die Aufgabe bearbeiten. Weitere Informationen finden Sie unter „**Eigenschaften konfigurieren**“ (S. 86).

Klicken Sie auf **Beenden**, um die zeitgesteuerte Aufgabe zu speichern.



Beachten Sie

Die neue Aufgabe wird nun im Abschnitt **Zeitgesteuerte Aufgaben** angezeigt.

Eigenschaften konfigurieren

Um eine vorhandene zeitgesteuerte Aufgabe zu bearbeiten oder um weitere Einstellungen zu konfigurieren, die nicht im Konfigurationsassistenten zur Verfügung stehen, doppelklicken Sie einfach auf die Aufgabe oder wählen Sie sie aus und klicken Sie auf **Eigenschaften**. Das Konfigurationsfenster wird erscheinen.

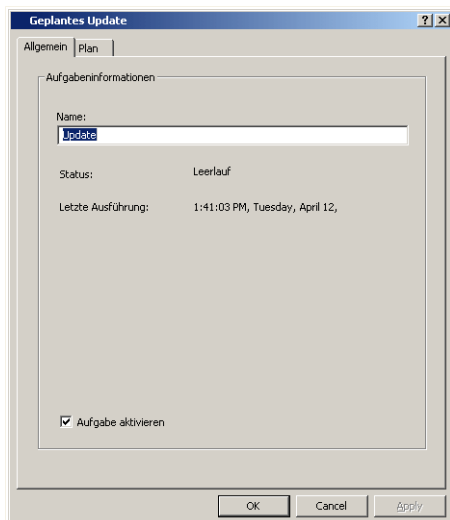


Beachten Sie

Um das Konfigurationsfenster zu öffnen, können Sie auch **Erweiterte Eigenschaften öffnen, wenn ich auf "Beenden" klicke** im letzten Schritt des Assistenten wählen.

Allgemeine Informationen betrachten

Öffnen Sie das Konfigurationsfenster, um allgemeine Informationen zu betrachten.



Allgemein

Hier finden Sie allgemeine Informationen über die Aufgabe (Name, Status und der letzte Zeitpunkt der Ausführung). Wenn Sie den Namen der Aufgabe ändern möchten, geben Sie einen neuen Namen in das entsprechende Feld ein.

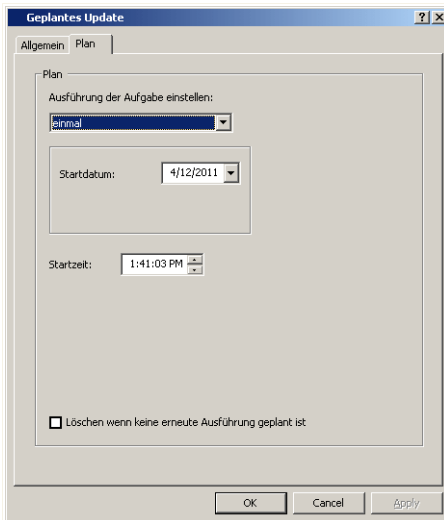
Um die Aufgabe zu aktivieren, wählen Sie **Aufgabe aktivieren**. Lassen Sie das Kontrollkästchen andererseits frei.

Klicken Sie auf **Anwenden**, um die Änderungen zu speichern. Wenn Sie die Änderungen speichern und das Konfigurationsfenster schließen möchten, klicken Sie auf **OK**.

Wenn das Konfigurationsfenster schließen möchten ohne die Änderungen zu speichern, klicken Sie auf **Abbrechen**.

Zeitsteuerung bearbeiten

Klicken Sie auf den Tab **Zeitsteuerung** im Konfigurationsfenster um die Zeitsteuerung zu bearbeiten.



Plan

Geben Sie den Zeitplan für die Aufgabe an.

Sie müssen eine der folgenden Optionen aus dem Menu wählen:

- **Einmal** - führt das Update nur einmal, zu einem bestimmten Zeitpunkt aus.

Geben Sie den Zeitpunkt des Starts und des Endes in die Felder **Startdatum/Ende** ein.

- **Periodisch** - führt die Aufgabe periodisch, in bestimmten zeitlichen Abständen (Minuten, Stunden, Tage, Wochen, Monate, Jahre) aus. Der Startpunkt wird mit Datum und Uhrzeit festgelegt.

Um die nötigen Einstellungen zu konfigurieren, befolgen Sie die folgenden Schritte:

1. Geben Sie das Startdatum in das Feld **Startdatum** ein.
2. Wenn Sie möchten, dass die Aufgabe mehrmals bis zu einem bestimmten Datum ausgeführt wird, markieren Sie **Ende** und geben Sie das Datum des Endes in das entsprechende Feld ein.
3. Geben Sie die Startzeit in das Feld **Startzeit** ein.
4. Legen Sie die Häufigkeit der Aufgabe fest, indem Sie in das entsprechende Feld die Anzahl der Minuten / Stunden / Tage / Wochen / Monate / Jahre angeben, die zwischen zwei Aufgaben liegen sollen.

- **Wochentage** - um die Aufgabe mehrmals an bestimmten Wochentagen auszuführen, wobei an einem festgelegten Datum/Uhrzeit begonnen wird.

Um die nötigen Einstellungen zu konfigurieren, befolgen Sie die folgenden Schritte:

1. Geben Sie das Startdatum in das Feld **Startdatum** ein.
2. Wenn Sie möchten, dass die Aufgabe mehrmals bis zu einem bestimmten Datum ausgeführt wird, wählen Sie **Ende** und geben Sie das Enddatum in das entsprechende Feld ein.
3. Geben Sie die Startzeit in das Feld **Startzeit** ein.
4. Wählen Sie den Tag oder die Tage an dem/denen die Aufgabe ausgeführt werden soll.

Wählen Sie **Löschen wenn keine erneute Ausführung geplant ist** - löscht die Aufgabe nach der letzten Ausführung.

Klicken Sie auf **Anwenden**, um die Änderungen zu speichern. Wenn Sie die Änderungen speichern und das Konfigurationsfenster schließen möchten, klicken Sie auf **OK**.

Wenn das Konfigurationsfenster schließen möchten ohne die Änderungen zu speichern, klicken Sie auf **Abbrechen**.

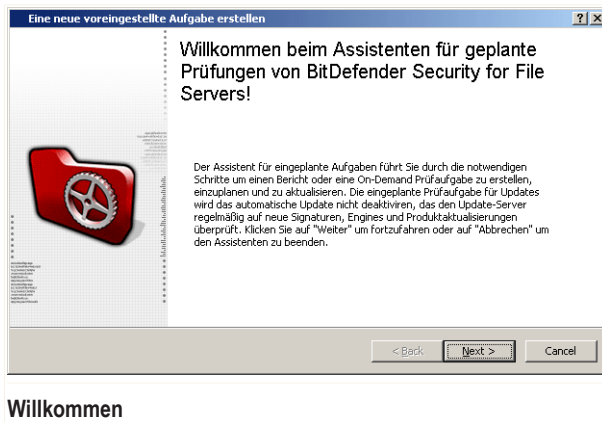
8.6.4. Aufgaben zur Berichterstellung

Aufgaben zeitlich einplanen

Sie erstellen eine neue zeitgesteuerte Aufgabe, indem Sie auf **Neue Aufgabe** klicken. Es erscheint ein Konfigurationsassistent, der Sie durch den Prozess der Erstellung einer zeitgesteuerten Aufgabe begleitet.

So richten Sie eine zeitgesteuerte Aufgabe zur Berichterstellung ein:

Schritt 1/7 - Willkommen zum Assistenten für zeitgesteuerte Aufgaben



Klicken Sie auf **Weiter**.

Schritt 2/7 – Aufgabentyp wählen

Auswählen des Aufgabentyps

Geben Sie den Namen der Aufgabe an und wählen Sie **Aufgabe zur Berichterstellung**.

Klicken Sie auf **Weiter**.

Schritt 3/7 – Zeitsteuerung konfigurieren

Konfigurieren Sie den Aufgabenplan.

Geben Sie den Zeitplan für die Aufgabe an.

Sie müssen eine der folgenden Optionen aus dem Menu wählen:

- **Einmal** - führt das Update nur einmal, zu einem bestimmten Zeitpunkt aus.

Geben Sie den Zeitpunkt des Starts und des Endes in die Felder **Startdatum/Ende** ein.

- **Periodisch** - führt die Aufgabe periodisch, in bestimmten zeitlichen Abständen (Minuten, Stunden, Tage, Wochen, Monate, Jahre) aus. Der Startpunkt wird mit Datum und Uhrzeit festgelegt.

Um die nötigen Einstellungen zu konfigurieren, befolgen Sie die folgenden Schritte:

1. Geben Sie das Startdatum in das Feld **Startdatum** ein.
2. Wenn Sie möchten, dass die Aufgabe mehrmals bis zu einem bestimmten Datum ausgeführt wird, markieren Sie **Ende** und geben Sie das Datum des Endes in das entsprechende Feld ein.
3. Geben Sie die Startzeit in das Feld **Startzeit** ein.
4. Legen Sie die Häufigkeit der Aufgabe fest, indem Sie in das entsprechende Feld die Anzahl der Minuten / Stunden / Tage / Wochen / Monate / Jahre angeben, die zwischen zwei Aufgaben liegen sollen.

- **Wochentage** - um die Aufgabe mehrmals an bestimmten Wochentagen auszuführen, wobei an einem festgelegten Datum/Uhrzeit begonnen wird.

Um die nötigen Einstellungen zu konfigurieren, befolgen Sie die folgenden Schritte:

1. Geben Sie das Startdatum in das Feld **Startdatum** ein.
2. Wenn Sie möchten, dass die Aufgabe mehrmals bis zu einem bestimmten Datum ausgeführt wird, wählen Sie **Ende** und geben Sie das Enddatum in das entsprechende Feld ein.
3. Geben Sie die Startzeit in das Feld **Startzeit** ein.
4. Wählen Sie den Tag oder die Tage an dem/denen die Aufgabe ausgeführt werden soll.

Klicken Sie auf **Weiter**.

Schritt 4/7 – Berichtstyp wählen



Wählen Sie eine der zur Verfügung stehenden Berichtstypen.

Berichtstyp	Beschreibung
Gesamt	Bietet umfangreiche Informationen über die Bedrohungen die innerhalb eines bestimmten Zeitraums entdeckt wurden.
Häufigste Viren	Bietet eine Tabelle mit den entdeckten Bedrohungen, die innerhalb eines bestimmten Zeitraums entdeckt wurden, geordnet nach der Anzahl der infizierten Dateien.

Klicken Sie auf **Weiter**.

Schritt 5/7 – Berichtsformat wählen



Wählen Sie das Berichtsformat

Wählen Sie das Format der Berichtsdatei (**HTML** oder **CSV**).

Klicken Sie auf **Weiter**.

Schritt 6/7 – Zeitintervall einstellen



Wählen Sie den Zeitraum aus

Wählen Sie den im Bericht bedeckten Zeitabstand aus:

- **Letzter Tag**
- **Letzte Woche**
- **Letzter Monat**
- **Benutzerdefiniert**

Wenn Sie Information über BitDefender mit einem spezifischen Zeitabstand verbundene Tätigkeit benötigen, wählen Sie **anpassen** und geben Sie das Beginn/Enddatum an.

Um das Startdatum und das Ende festzulegen, klicken Sie entweder auf die Datumsfelder und geben Sie neue Werte ein oder klicken Sie auf **den Pfeil** um ein Datum aus dem Kalender zu wählen.

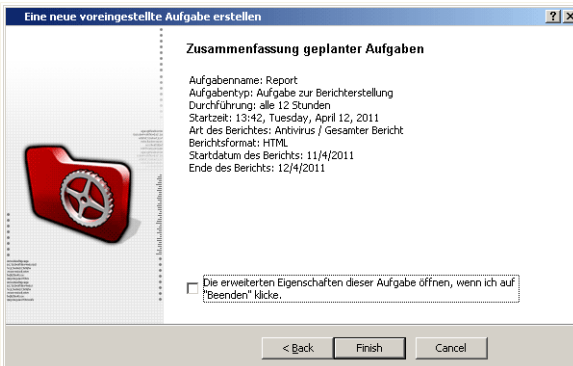


Beachten Sie

Das Format des Datums ist Monat/Tag/Jahr.

Nur Aufnahmen aus dem festgelegten Zeitraum werden in dem Bericht erscheinen.
Klicken Sie auf **Weiter**.

Schritt 7/7 – Zusammenfassung betrachten



Betrachten Sie die Zusammenfassung

In diesem Fenster können Sie die Aufgabeneinstellungen überprüfen. Sie können Änderungen vornehmen, indem Sie zu den vorherigen Schritten zurückkehren (klicken Sie auf **Zurück**).

Wählen Sie **Erweiterte Eigenschaften dieser Aufgabe öffnen, wenn ich auf "Beenden" klicke** wenn Sie möchten, dass das Fenster **Eigenschaften** dieser Aufgabe geöffnet wird, wenn Sie den Assistenten beenden. In diesem Fenster können Sie die weitere Einstellungen konfigurieren und die Aufgabe bearbeiten. Weitere Informationen finden Sie unter „**Eigenschaften konfigurieren**“ (S. 94).

Klicken Sie auf **Beenden**, um die zeitgesteuerte Aufgabe zu speichern.



Beachten Sie

Die neue Aufgabe wird nun im Abschnitt **Zeitgesteuerte Aufgaben** angezeigt.

Eigenschaften konfigurieren

Um eine vorhandene zeitgesteuerte Aufgabe zu bearbeiten oder um weitere Einstellungen zu konfigurieren, die nicht im Konfigurationsassistenten zur Verfügung

stehen, doppelklicken Sie einfach auf die Aufgabe oder wählen Sie sie aus und klicken Sie auf **Eigenschaften**. Das Konfigurationsfenster wird erscheinen.

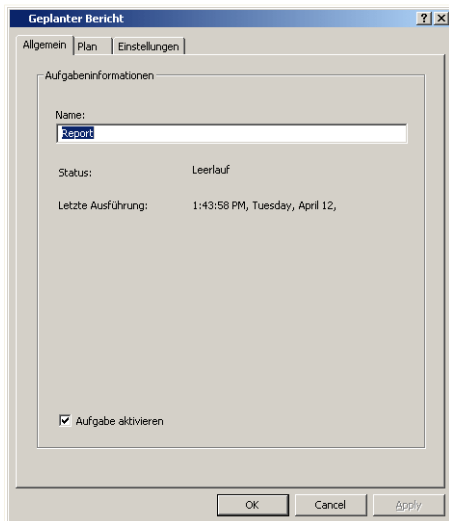


Beachten Sie

Um das Konfigurationsfenster zu öffnen, können Sie auch **Erweiterte Eigenschaften öffnen, wenn ich auf "Beenden" klicke** im letzten Schritt des Assistenten wählen.

Allgemeine Informationen betrachten

Öffnen Sie das Konfigurationsfenster, um allgemeine Informationen zu betrachten.



Allgemein

Hier finden Sie allgemeine Informationen über die Aufgabe (Name, Status und der letzte Zeitpunkt der Ausführung). Wenn Sie den Namen der Aufgabe ändern möchten, geben Sie einen neuen Namen in das entsprechende Feld ein.

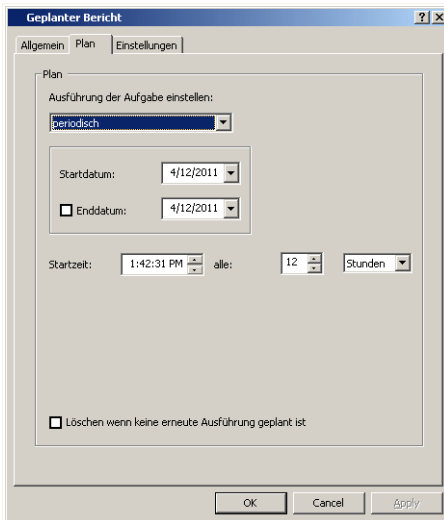
Um die Aufgabe zu aktivieren, wählen Sie **Aufgabe aktivieren**. Lassen Sie das Kontrollkästchen andererseits frei.

Klicken Sie auf **Anwenden**, um die Änderungen zu speichern. Wenn Sie die Änderungen speichern und das Konfigurationsfenster schließen möchten, klicken Sie auf **OK**.

Wenn das Konfigurationsfenster schließen möchten ohne die Änderungen zu speichern, klicken Sie auf **Abbrechen**.

Zeitsteuerung bearbeiten

Klicken Sie auf den Tab **Zeitsteuerung** im Konfigurationsfenster um die Zeitsteuerung zu bearbeiten.



Plan

Geben Sie den Zeitplan für die Aufgabe an.

Sie müssen eine der folgenden Optionen aus dem Menu wählen:

- **Einmal** - führt das Update nur einmal, zu einem bestimmten Zeitpunkt aus.

Geben Sie den Zeitpunkt des Starts und des Endes in die Felder **Startdatum/Ende** ein.

- **Periodisch** - führt die Aufgabe periodisch, in bestimmten zeitlichen Abständen (Minuten, Stunden, Tage, Wochen, Monate, Jahre) aus. Der Startpunkt wird mit Datum und Uhrzeit festgelegt.

Um die nötigen Einstellungen zu konfigurieren, befolgen Sie die folgenden Schritte:

1. Geben Sie das Startdatum in das Feld **Startdatum** ein.
2. Wenn Sie möchten, dass die Aufgabe mehrmals bis zu einem bestimmten Datum ausgeführt wird, markieren Sie **Ende** und geben Sie das Datum des Endes in das entsprechende Feld ein.
3. Geben Sie die Startzeit in das Feld **Startzeit** ein.
4. Legen Sie die Häufigkeit der Aufgabe fest, indem Sie in das entsprechende Feld die Anzahl der Minuten / Stunden / Tage / Wochen / Monate / Jahre angeben, die zwischen zwei Aufgaben liegen sollen.

- **Wochentage** - um die Aufgabe mehrmals an bestimmten Wochentagen auszuführen, wobei an einem festgelegten Datum/Uhrzeit begonnen wird.

Um die nötigen Einstellungen zu konfigurieren, befolgen Sie die folgenden Schritte:

1. Geben Sie das Startdatum in das Feld **Startdatum** ein.
2. Wenn Sie möchten, dass die Aufgabe mehrmals bis zu einem bestimmten Datum ausgeführt wird, wählen Sie **Ende** und geben Sie das Enddatum in das entsprechende Feld ein.
3. Geben Sie die Startzeit in das Feld **Startzeit** ein.
4. Wählen Sie den Tag oder die Tage an dem/denen die Aufgabe ausgeführt werden soll.

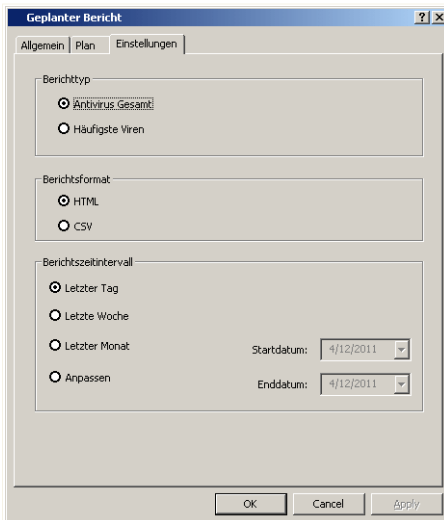
Wählen Sie **Löschen wenn keine erneute Ausführung geplant ist** - löscht die Aufgabe nach der letzten Ausführung.

Klicken Sie auf **Anwenden**, um die Änderungen zu speichern. Wenn Sie die Änderungen speichern und das Konfigurationsfenster schließen möchten, klicken Sie auf **OK**.

Wenn das Konfigurationsfenster schließen möchten ohne die Änderungen zu speichern, klicken Sie auf **Abbrechen**.

Einstellungen konfigurieren

Klicken Sie auf den Tab **Einstellungen** im Konfigurationsfenster, um die Berichtseinstellungen zu bearbeiten.



Einstellungen

Befolgen Sie diese Schritte, um die Berichtseinstellungen zu konfigurieren:

1. Wählen Sie eine der zur Verfügung stehenden Berichtstypen.

Berichtstyp	Beschreibung
Gesamt	Bietet umfangreiche Informationen über die Bedrohungen die innerhalb eines bestimmten Zeitraums entdeckt wurden.
Häufigste Viren	Bietet eine Tabelle mit den entdeckten Bedrohungen, die innerhalb eines bestimmten Zeitraums entdeckt wurden, geordnet nach der Anzahl der infizierten Dateien.

2. Wählen Sie das Format der Berichtdatei (**HTML** oder **CSV**).
3. Wählen Sie den im Bericht bedeckten Zeitabstand aus:
 - **Letzter Tag**
 - **Letzte Woche**
 - **Letzter Monat**
 - **Benutzerdefiniert**

Klicken Sie auf **Anwenden**, um die Änderungen zu speichern. Wenn Sie die Änderungen speichern und das Konfigurationsfenster schließen möchten, klicken Sie auf **OK**.

Wenn das Konfigurationsfenster schließen möchten ohne die Änderungen zu speichern, klicken Sie auf **Abbrechen**.

9. Serverprüfung

Serverprüfung - die Art wie BitDefender den File Server überprüft kann konfiguriert werden.

BitDefender Security for File Server schützt auf Windows basierende Server vor verschiedenen Arten von Schädlingen (Virus, Spyware, Adware, Rootkits und so weiter). Das Produkt bietet zwei Schutzebenen:

- **Echtzeitschutz** - hält den Benutzer davon ab, infizierte Dateien zu öffnen oder kopieren, damit diese nicht im Netzwerk verbreitet werden. BitDefender prüft Dateien wenn auf diese zugegriffen wird oder Sie auf die Festplatte kopiert werden entsprechend der eingestellten Sicherheitsstufe. Die Aktionen, die durchgeführt werden sollen, falls infizierte oder verdächtige Dateien entdeckt werden, hängen ebenfalls von der eingestellten Sicherheitsstufe ab.

Standardmäßig ist der Echtzeitschutz auf **Mittel** eingestellt, was einen gute Virentdeckung bei niedrigem Ressourcenverbrauch gewährleistet. BitDefender ist so konfiguriert, dass infizierte Dateien desinfiziert werden (der Zugriff wird verweigert falls die Desinfektion fehlschlägt) und verdächtigen Dateien der Zugriff verweigert wird. Um die Sicherheitsstufe zu ändern oder den Echtzeitschutz vollständig zu personalisieren, öffnen Sie den Tab **Echtzeit**.



Beachten Sie

Der Echtzeitschutz gilt auch für die Prüfung auf Zugriff (On-Access) - Dateien werden geprüft, sobald die Benutzer auf sie zugreifen.

- **On-demand Prüfung** - erkennt und entfernt Malware die sich bereits auf dem System befindet. Hierbei handelt es sich um eine klassische, durch den Administrator gestartete, Prüfung - Sie wählen das Laufwerk, Ordner oder Datei welche BitDefender prüfen soll, und BitDefender prüft diese auf Anfrage.

Um einen On-Demand Prüfvorgang zu konfigurieren und zu starten öffnen Sie den Tab **Prüfaufgaben**. Sie können verschiedene Prüfmodi durchführen. Wählen Sie den Benutzermodus um die Prüfoptionen und die Locations, die geprüft werden sollen, vollständig zu konfigurieren.

Sie können Dateien und Ordner auch ganz leicht über die Option **Mit BitDefender prüfen** aus dem Window-Kontextmenü prüfen.

Sie können On-Demand Prüfaufgaben so einstellen, dass Sie zu einem bestimmten Zeitpunkt und regelmäßig durchgeführt werden. Für weitere Informationen lesen Sie bitte „**Geplante Aufgaben**“ (S. 62).

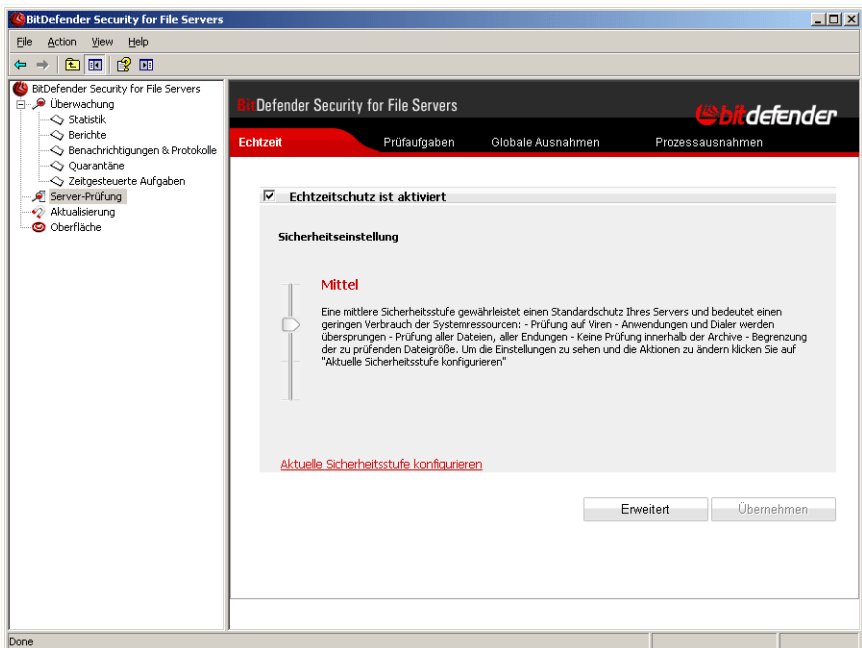
Je nach der Configuration des Systems, auf dem BitDefender Security for File Server installiert ist, sind während der Installation bestimmte Dateien und Ordner automatisch vom Scan ausgeschlossen. Stellen Sie fest welche Dateien, Ordner oder Prozesse, die Sie nicht prüfen möchten. Weitere Informationen finden Sie unter „**Prüfausnahmen**“ (S. 129).

9.1. Echtzeitschutz

Der Echtzeitschutz schützt den File Server vor neuen Viren, Spyware und Riskware. Es hält Benutzer ebenfalls davon ab, auf infizierte Dateien zuzugreifen oder diese zu kopieren, weshalb einer Virenverbreitung im Netzwerk vorgebeugt wird.

BitDefender prüft Dateien wenn auf sie zugegriffen wird oder sie kopiert werden, entsprechend der eingestellten Sicherheitsstufe. Die Aktionen, die durchgeführt werden sollen, falls infizierte oder verdächtige Dateien entdeckt werden, hängen ebenfalls von der eingestellten Sicherheitsstufe ab.

Um den Echtzeitschutz zu konfigurieren, klicken Sie auf **Serverprüfung** im Baummenu und dann auf den Tab **Echtzeit**.



Echtzeitschutz

Der Echtzeitschutz ist standardmäßig aktiviert. Wenn Sie ihn deaktivieren möchten, lassen Sie das Kontrollkästchen **Echtzeitschutz ist aktiviert** frei und klicken Sie auf **Anwenden**.



Wichtig

Lassen Sie den Echtzeitschutz aktiviert um den File Server und die Arbeitsplätze vor Viren, Spyware und anderer Malware zu schützen.

9.1.1. Sicherheitsstufe einstellen

Mit der Sicherheitsstufe können Sie den Echtzeitschutz konfigurieren, indem Sie die Standardeinstellungen oder benutzerdefinierte Einstellungen verwenden. Die durchzuführenden Aktionen für entdeckte Dateien die infiziert oder verdächtig sind sind für jede Sicherheitsstufe konfigurierbar.

Wählen Sie mithilfe des Schiebers die Sicherheitsstufe, die Ihren Bedürfnissen am Besten entspricht. Folgende 4 Sicherheitsstufen sind wählbar:

Sicherheitseinstellung	Beschreibung
Hoch	Gewährleistet hohe Sicherheit. Mittlere Belastung der Ressourcen. • Prüft alle Dateien auf die zugegriffen wird, unabhängig von deren Endung und Größe. Die Bootsektoren der verfügbaren Laufwerke werden ebenfalls geprüft. • Dateien, auf die zugegriffen wird, werden auf alle Malware-Typen überprüft (Virus, Trojaner, Spyware, Adware, Rootkits, Dialers und so weiter). • BitDefender überprüft den Inhalt von Archiven. • Die Standardaktion für infizierte Dateien lautet Desinfizieren. Wenn die Desinfektion fehlschlägt, wird die infizierte Datei gelöscht. • Die Standardaktion für verdächtige Dateien lautet Löschen.
Mittel	Gewährleistet Standard Sicherheit. Belastung der Ressourcen ist gering. • Nur Dateien auf die zugegriffen wird und die eine Größe von 10 MB nicht überschreiten werden geprüft. Die Bootsektoren der verfügbaren Laufwerke werden ebenfalls geprüft. • Dateien auf die zugegriffen wird werden nur auf Viren, Trojaner und Spyware überprüft. • BitDefender prüft nicht den Inhalt von Archiven. • Die Standardaktion für infizierte Dateien lautet Desinfizieren. Wenn die Desinfektion fehlschlägt, wird der Zugriff auf solche Dateien verweigert. • Die Standardeinstellung für verdächtige Dateien lautet Zugriff verweigern.
Niedrig	Deckt einfache Anforderungen ab. Geringe Belastung der Ressourcen. • Nur die Anwendungsdateien auf die zugegriffen wird und die 5 MB nicht überschreiten werden geprüft.

Sicherheitseinstellung	Beschreibung
	• Dateien auf die zugegriffen wird werden nur auf Viren, Trojaner und Spyware überprüft. • BitDefender prüft nicht den Inhalt von Archiven. • Die Standardaktion für infizierte Dateien lautet Desinfizieren. Wenn die Desinfektion fehlschlägt, wird der Zugriff auf solche Dateien verweigert. • Die Standardeinstellung für verdächtige Dateien lautet Zugriff verweigern.
Benutzerdefiniert	Die Einstellungen des Echtzeitschutzes können angepasst werden. Um diese Einstellungen zu konfigurieren klicken sie auf Aktuelle Sicherheitsstufe konfigurieren .

Um die Einstellungen einer Sicherheitsstufe detailliert zu betrachten:

1. Bewegen Sie den Schieberegler, um die entsprechende Stufe einzustellen.
2. Klicken Sie auf **Aktuelle Sicherheitsstufe konfigurieren** um das Konfigurationsfenster zu öffnen.
3. Klicken Sie auf die Tabs um die konfigurierten Prüfeinstellungen, Aktionen und Benachrichtigungen zu sehen.

Klicken Sie nachdem Sie die neue Sicherheitsstufe eingestellt haben auf **Anwenden**, um die Änderungen zu speichern.

9.1.2. Sicherheitsstufe einstellen

Für jede Sicherheitsstufe können die Aktionen konfiguriert werden, die für infizierte und verdächtige Dateien durchgeführt werden sollen sowie die Ereignisbenachrichtigung für den Echtzeitschutz. Wenn Sie die Prüfeinstellungen ebenfalls konfigurieren möchten, verwenden Sie die Stufe **Benutzerdefiniert**.

Um die aktuellen Einstellungen der Sicherheitsstufe zu konfigurieren:

1. Klicken sie auf **Aktuelle Sicherheitsstufe konfigurieren**. Das Konfigurationsfenster wird erscheinen.
2. Klicken sie auf die Tabs und konfigurieren Sie die entsprechenden Einstellungen wie gewünscht.
3. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.

Das Konfigurationsfenster hat zwei Tabs:

Tab	Beschreibung
Prüfeinstellungen	In diesem Tab können Sie die Prüfeinstellungen des Echtzeitschutzes einstellen. Sie können BitDefender so einstellen, dass nur Dateien mit bestimmten Endungen geprüft werden oder das bestimmte Dateiformate, Archive oder Dateien, die eine bestimmte Größe überschreiten von der Prüfung ausgelassen werden.
Aktionen	In diesem Tab können Sie die Aktionen für entdeckte Dateien die infiziert oder verdächtig sind auswählen.
Benachrichtigungen	In diesem Tab können Sie die Ereignisse der On-Access Prüfung festlegen, über die BitDefender Sie benachrichtigen soll.

Tab Prüfeinstellungen

In diesem Tab können Sie die Prüfeinstellungen des Echtzeitschutzes einstellen.



Beachten Sie

Diese Einstellungen können nur dann konfiguriert werden, wenn Sie die Sicherheitsstufe **Benutzerdefiniert** ausgewählt haben.

Echtzeit-Schutz Einstellungen

Auswählen | Einstellungen | Aktionen | Benachrichtigungen

Prüfziel

- ☒ Alle Dateien prüfen
 - Benutzerdefinierte Prüfung
 - Fügen Sie Dateien und Ordner hier hinzu (Platzhalter werden akzeptiert). Klicken Sie auf das Eingabefeld und beginnen Sie mit der Eingabe, indem Sie jede Datei und jeden Ordner mit der Eingabetaste, einem Komma oder einem Strichpunkt trennen. Sie können auch mit Kopieren/Einfügen arbeiten oder sie aus einer Textdatei importieren.
- ☐ Nur Anwendungsdateien prüfen
- ☐ Benutzerdefinierte Endungen prüfen
- ☐ Alle Dateien bis auf die folgenden Endungen prüfen

Importieren...
Exportieren...
Durchsuchen

Filter

- ☒ Alle Endungen prüfen
- ☐ Nur Anwendungsdateien prüfen
- ☐ Benutzerdefinierte Endungen prüfen
- ☐ Alle Dateien bis auf die folgenden Endungen prüfen

Maximale Dateigröße für die Prüfung: 10000 KB

Erweitert

OK Cancel Apply

Tab Prüfeinstellungen

Mit den Prüfeinstellungen von BitDefender, können Sie den Echtzeitschutz den Anforderungen Ihres Unternehmens, bezüglich der Sicherheit Ihres File Servers, anpassen. Der Echtzeitschutz kann wie folgt konfiguriert werden:

- um nur Dateien an bestimmten Locations des File Servers zu prüfen.
- um nur Dateien mit bestimmten Endungen zu prüfen oder bestimmte Dateiformate nicht zu prüfen.
- um Dateien nicht zu prüfen die eine festgelegte Größe überschreiten.
- um Archive nicht zu prüfen.
- um spezielle Dateien und Ordner nicht zu prüfen.

Durch diese Feineinstellungen kann die Prüfzeit erheblich reduziert werden und die Leistung des Systems während des Scans wird verbessert.

Festlegen der Zielobjekte

Standardmäßig prüft BitDefender Dateien auf die zugegriffen wird unabhängig von deren Location auf dem File Server. Auf diese Weise wird der gesamte File Server vor Viren und Spyware geschützt.

Wenn Sie möchten, dass nur Dateien die sich in bestimmten Locations befinden geprüft werden sollen, befolgen Sie die folgenden Schritte:

1. Wählen Sie **Benutzerdefinierte Prüfung**.
2. Wählen Sie eine der folgenden Methoden:
 - Geben Sie in das Editierfeld den vollständigen Pfad der zu prüfenden Dateien und Ordner ein, wobei Sie diese mit der Eingabetaste, einem Komma oder Strichpunkt trennen müssen.
 - Klicken Sie auf **Durchsuchen** und wählen Sie die zu prüfenden Dateien und Ordner.
 - Wenn Sie über eine Textdatei verfügen, die eine Liste der Locations (von Dateien und Ordnern) enthält, die geprüft werden sollen, klicken Sie auf **Importieren** und laden Sie die entsprechende Datei. Sie können die Locations auch aus der Textdatei kopieren und direkt in das Editierfeld einfügen.

Um die Liste der Dateien und Ordner als eine Textdatei zu speichern, klicken Sie auf **Exportieren**.

Dateien anhand der Endungen prüfen

Bestimmte Dateisorten sind anfälliger auf Viren als andere. So ist zum Beispiel das Risiko beim Ausführen einer `.exe` Datei höher, als beim Öffnen einer `.txt` oder einer `.gif` Datei.

Um festzulegen welche Dateisorten geprüft werden sollen, wählen Sie zwischen den folgenden Optionen wählen:

Optionen	Beschreibung
Alle Endungen prüfen	Alle Dateien auf die zugegriffen wird werden unabhängig von ihrem Typ geprüft.
Nur Anwendungsdateien prüfen	Nur Anwendungsdateien werden geprüft. Diese Kategorie ist auf Dateien mit den folgenden Erweiterungen beschränkt: 386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsd; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp Viren werden normalerweise über Anwendungsdateien übertragen. Deswegen sollten diese Dateiarten immer bei Zugriff geprüft werden.
Benutzerdefinierte Endungen prüfen	Nur Dateien mit den festgelegten Endungen werden geprüft. Sie müssen in das Editierfeld die Dateieendungen eingeben, die von BitDefender geprüft werden sollen, wobei diese mit Strichpunkten (",") zu trennen sind.
Alle bis auf die folgenden Endungen prüfen	Die Dateien mit den festgelegten Endungen werden NICHT geprüft. Sie müssen in das Editierfeld die Dateieendungen eingeben, die NICHT von BitDefender geprüft werden sollen, wobei diese mit Strichpunkten (",") zu trennen sind. Sie sollten Dateiarten, die bekannt für Vren sind nicht von der Prüfung ausschließen, wie beispielsweise .exe, .doc, .ppt, .xls, .rtf, .pif, .bat und Andere.

Dateien anhand der Größe prüfen.

Die Prüfung großer Dateien erfordert zusätzliche Systemressourcen, was das System verlangsamt.

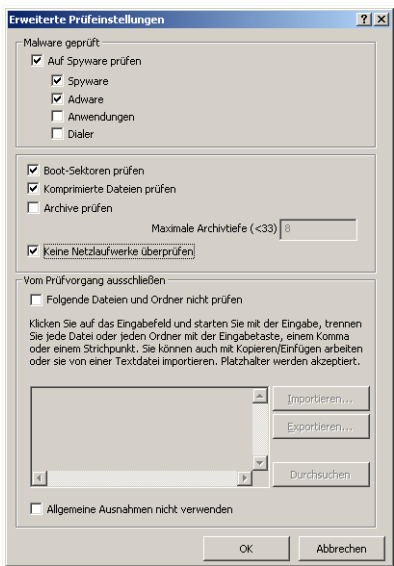
Legen Sie das Größenlimit (in KB) der zu prüfenden Dateien in dem Feld **Maximale Größe von zu prüfenden Dateien** fest. Wenn Sie beispielsweise 2000 eingeben, werden alle Dateien die größer als 2000 KB sind von der Prüfung ausgeschlossen.

Wenn Sie alle Dateien auf die zugegriffen wird, unabhängig von deren Größe, prüfen möchten, befolgen Sie eine der folgenden Möglichkeiten:

- Lassen Sie das Kontrollkästchen zu **Maximale Größe von zu prüfenden Dateien** frei.
- Geben Sie als Größenbegrenzung 0 KB ein.

Weitere Einstellungen und Ausnahmen konfigurieren

Um weitere Einstellungen vorzunehmen oder Ausnahmen der On-Access-Prüfung festzulegen klicken Sie auf **Erweitert**. Ein neues Konfigurationsfenster wird sich öffnen.



Mehr Einstellungen

Folgende erweiterte Prüfeinstellungen können konfiguriert werden:

Optionen	Beschreibung
Malware geprüft	Dateien beim Zugriff nicht nur auf Viren sondern auch auf bekannte Riskware überprüfen. Die Kategorie Riskware

Optionen	Beschreibung
	beinhaltet Spyware, Adware, Dialers und andere Anwendungen, die zu schädlichen Zwecken verwendet werden können. Erkannte Dateien werden als infiziert behandelt. Software welche diese Dateien verwendet könnte Ihre Arbeit einstellen falls diese Option aktiviert ist.
Boot-Sektoren	Den Bootsektor der verfügbaren Laufwerke prüfen.
Komprimierte Dateien prüfen	Komprimierte Dateien prüfen.
Netzwerkfreigaben nicht prüfen	BitDefender wird keine Netzwerkfreigaben auf dem File Server prüfen um einen schnelleren Netzwerkzugriff zu erlauben. Wir empfehlen die Aktivierung dieser Option nur wenn auf den anderen Netzwerkrechnern ebenfalls eine Antiviruslösung installiert ist.
Archive prüfen	Archivierte Dateien prüfen. Sie können eine maximale Archivtiefe festlegen, um Dateien zu prüfen, die mehrfach archiviert wurden. Wenn Sie Dateien prüfen wollen, egal wie häufig diese archiviert wurden, stellen Sie die maximale Archivtiefe auf 0 ein. Durch wählen dieser Option wird die Leistung des Systems verlangsamt.

Um Dateien und Ordner nur von der Prüfung On-Access auszuschließen:

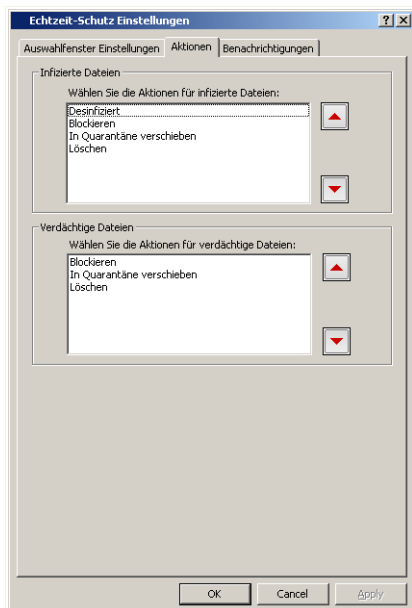
1. Wählen Sie **Folgende Dateien und Ordner nicht prüfen**.
2. Wählen Sie eine der folgenden Methoden:
 - Geben Sie in das Editierfeld den vollständigen Pfad der Dateien und Ordner ein, die nicht geprüft werden sollen, wobei Sie diese mit der Eingabetaste, einem Komma oder Strichpunkt trennen müssen.
 - Klicken Sie auf **Durchsuchen** und wählen Sie die Dateien und Ordner, die nicht geprüft werden sollen.
 - Wenn Sie über eine Textdatei verfügen, die eine Liste der Locations (von Dateien und Ordnern) enthält, die nicht geprüft werden sollen, klicken Sie auf **Importieren** und laden Sie die entsprechende Datei. Sie können die Locations auch aus der Textdatei kopieren und direkt in das Editierfeld einfügen.

Um die Liste der Dateien und Ordner als eine Textdatei zu speichern, klicken Sie auf **Exportieren**. Auf diese Weise können Sie diese Liste auf andere File Server laden, um die Prüfausnahmen zu konfigurieren.

Sie können ebenfalls festlegen, ob die allgemeinen Ausnahmen unter dem Abschnitt **Ausnahmen** für die Echtzeitprüfung angewendet werden.

Tab Aktionen

In diesem Tab können Sie die Aktionen für entdeckte Dateien die infiziert oder verdächtig sind auswählen.



Tab Aktionen

Sie können verschiedene Aktionen für verdächtige und infizierte Dateien festlegen. Es gibt eine Aktionsliste die für jede Kategorie entdeckter Dateien angewendet werden kann (infiziert oder verdächtig). Wenn eine infizierte Datei entdeckt wird, so wird die erste Aktion auf der entsprechenden Liste angewendet. Wenn diese Aktion fehlschlägt, wird die nächste Aktion angewendet, usw.

Sie können die Reihenfolge, in der die Aktionen angewendet werden verändern. Wählen Sie eine Aktion und klicken Sie auf  oder  um sie in der Liste nach oben oder nach unten zu verschieben.

Aktionen für infizierte Dateien. Folgende Aktionen stehen für infizierte Dateien zur Verfügung:

Aktion	Beschreibung
Desinfizieren	Den Malware-Code aus den angefragten infizierten Dateien vor Versendung entfernen. Die Wiederherstellung kann in einigen Fällen fehlschlagen (wenn die Datei z. B. innerhalb eines

Aktion	Beschreibung
	bestimmten Archivs ist oder sie von einem laufenden Prozess verwendet wird).
Verweigern	Den Benutzerzugriff auf angefragte Dateien verweigern, wenn BitDefender diese als infiziert entdeckt hat.
In Quarantäne verschieben	Infizierte Dateien von Ihrer ursprünglichen Position in den Quarantäne-Ordner verschieben. Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht kein Infektionsrisiko?
Löschen	Infizierte Dateien direkt und ohne Warnung von der Festplatte entfernen.

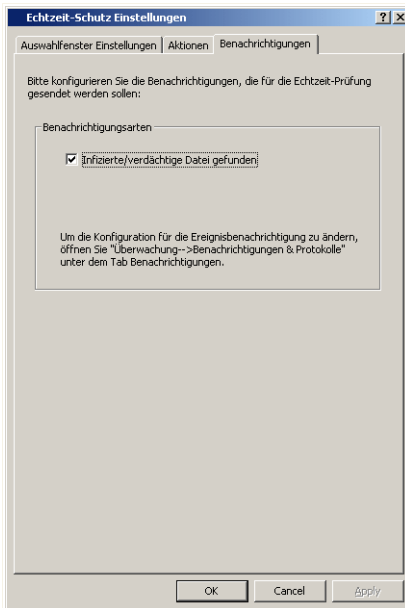
Aktionen für verdächtige Dateien. Folgende Aktionen stehen für verdächtige Dateien zur Verfügung:

Aktion	Beschreibung
Verweigern	Den Benutzerzugriff auf angefragte Dateien verweigern, wenn BitDefender diese als verdächtig identifiziert hat.
In Quarantäne verschieben	Verdächtige Dateien von der ursprünglichen Position in den Quarantäne-Ordner verschieben. Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht kein Infektionsrisiko?
Löschen	Verdächtige Dateien direkt und ohne Warnung von der Festplatte entfernen.

Wenn Sie möchten, dass BitDefender verdächtige Dateien automatisch zum BitDefender Labor für weitere Analysen sendet, wählen Sie das entsprechende Kontrollkästchen.

Tab Benachrichtigungen

BitDefender kann so eingestellt werden, dass Sie über bestimmte Ereignisse während des Betriebs benachrichtigt werden. In diesem Tab können Sie die Ereignisse der On-Access Prüfung festlegen, über die BitDefender Sie benachrichtigen soll.



Tab Benachrichtigungen

Wählen Sie die Ereignisse, über die Sie informiert werden möchten:

- **Infizierte/verdächtige Datei gefunden** - wenn eine infizierte oder verdächtige Datei gefunden wurde.
- **Datei nicht geprüft** - wenn eine Datei nicht geprüft werden konnte.

Um Bitdefender so zu konfigurieren, dass nur das Auftreten eines Ereignisses protokolliert wird oder dass Sie oder andere Personen über Net Send oder eine Mail darüber informiert werden, öffnen Sie das Modul **Benachrichtigungen&Protokolle** im Tab **Benachrichtigungen** und konfigurieren Sie das entsprechende Ereignis. Weitere Informationen finden Sie hier: *„Ereignisbenachrichtigung konfigurieren“* (S. 53).

9.1.3. Anzahl der Prüfinstanzen konfigurieren

Wenn Sie die Anzahl der zuvor konfigurierten Prüfinstanzen während der Installation ändern möchten, klicken Sie auf **Erweitert**. Ein neues Fenster wird sich öffnen.



Tippen Sie einen neuen Wert das Feld und der Klick **OK** ein, um die Änderungen zu speichern.

9.2. Prüfvorgang

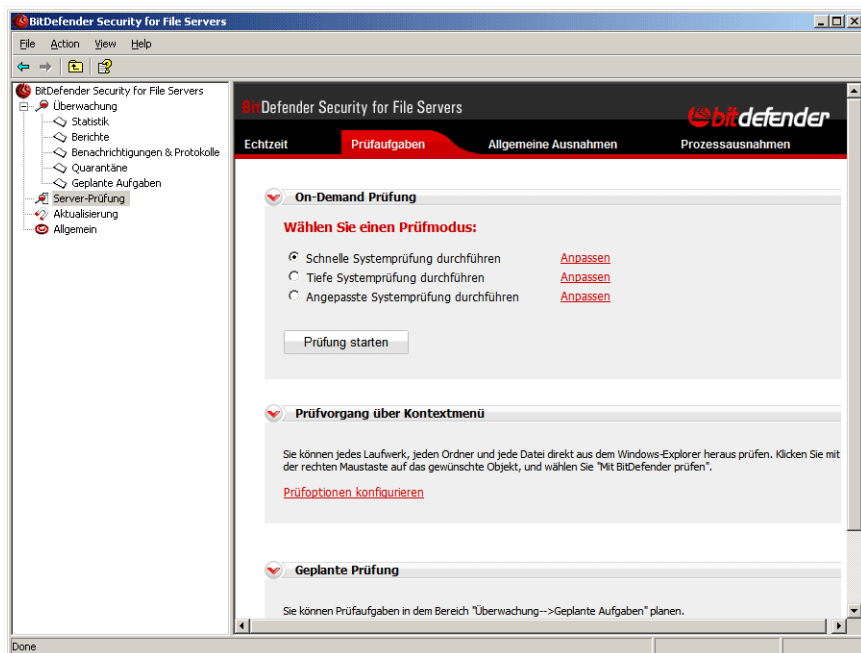
Die On-Demand-Prüfung bietet eine weitere Schutzebene für den File Server. Sie sollten den File Server von Zeit zu Zeit prüfen um sicherzustellen, dass er von Bedrohungen durch Malware frei ist (Viren, Spyware oder Rootkits). Es wird empfohlen jede Woche eine umfangreiche Systemprüfung durchzuführen.



Wichtig

Gleich nach der Installation des BitDefender Security for File Servers, führen Sie eine On-Demand Prüfung um irgendwelche Infektionen, die sich bereits auf Ihrem Computer befinden, zu entdecken bsw. zu löschen.

Um einen On-Demand-Prüfvorgang zu konfigurieren oder zu starten klicken Sie im Baummenu auf **Serverprüfung** und dann auf den Tab **Prüfaufgaben**.



Prüfaufgaben

Die On-Demand-Prüfung basiert auf den Prüfmodi. Ein Prüfmodus legt folgendes fest:

- die zu prüfenden Orte (Laufwerke, Ordner, Dateien).
- die Prüfeinstellungen.
- die vom Prüfvorgang ausgeschlossenen Objekte.
- die Aktionen für entdeckte Dateien die infiziert, verborgen oder verdächtig sind.

Sie können folgende Prüfmodi wählen:

Prüfmodus	Beschreibung
Schnelle Systemprüfung	Hier können die Ordner Programmdateien und Windows mithilfe einer festgelegten Konfiguration der Prüfeinstellungen schnell geprüft werden. Bitte beachten sie, dass nur Anwendungsdateien gespeichert werden, die eine Größe von 10 MB nicht überschreiten. Standardmäßig ist BitDefender so konfiguriert, dass folgende Aktionen durchgeführt werden:

Prüfmodus	Beschreibung
	• Desinfizieren - desinfiziert infizierte Dateien und Rootkits (versteckte Objekte). Wenn die Desinfektion fehlschlägt, werden die infizierten Dateien in die Quarantäne verschoben. • In Quarantäne verschieben für verdächtige Dateien.
Tiefgehende Systemprüfung	Bietet eine umfangreiche Prüfung des gesamten File Servers. Durch die voreingestellten Prüfeinstellungen wird die höchste Effizienz bei der Virenentdeckung gewährleistet. Standardmäßig ist BitDefender so konfiguriert, dass folgende Aktionen durchgeführt werden: • Desinfizieren - desinfiziert infizierte Dateien und Rootkits (versteckte Objekte). Wenn die Desinfektion fehlschlägt, werden die infizierten Dateien in die Quarantäne verschoben. • In Quarantäne verschieben für verdächtige Dateien.
Prüfung anpassen	Bietet die Möglichkeit bestimmte Ordner auf dem File Server zu prüfen, indem eine benutzerdefinierte Konfiguration der Prüfeinstellungen angewendet wird. Um diese Einstellungen zu konfigurieren, klicken Sie auf Anpassen.

9.2.1. Dateien und Ordner prüfen

Hier einige Tipps zur On-Demand-Prüfung:

- Vermeiden Sie die Prüfung des File Servers, wenn der Server ausgelastet ist, vor allem im Falle einer vollständigen Prüfung. Es wird empfohlen Prüfungen durchzuführen wenn der Server vollkommen oder fast unausgelastet ist. Beispielsweise sollten Sie tiefgehende Systemprüfungen Nachts oder am Wochenende durchführen (planen).
- Bevor Sie die Prüfung starten sollten Sie BitDefender aktualisieren damit das Programm die aktuellste Malware entdecken kann. Um BitDefender unverzüglich zu aktualisieren, befolgen Sie die folgenden Schritte:
 1. Klicken Sie im Baummenu auf **Update**.
 2. Klicken Sie auf den Tab **Update**.
 3. Click **Jetzt Updaten** .

Wenn Sie eine voreingestellte Prüfaufgabe für eine regelmäßige Ausführung eingestellt haben, so sollten Sie ebenfalls eine voreingestellte Update-Aufgabe konfigurieren, die wenige Minuten vor der Prüfung ausgeführt wird.



Wichtig

Wenn Sie das automatische Update deaktiviert haben oder die Häufigkeit von Updates niedrig ist, so ist die Aktualisierung von BitDefender vor der Prüfung ein MUSS.

- Führen Sie einmal pro Woche eine tiefgehende Systemprüfung durch um sicherzugehen, dass sich keine Malware auf Ihrem System befindet. Stellen Sie zu diesem Zweck in geeigneter Weise eine wöchentliche On-Demand-Prüfung ein. Für weitere Informationen lesen Sie bitte „*Geplante Aufgaben*“ (S. 62).

Es gibt 3 Möglichkeiten, eine On-Demand-Prüfung zu starten:

- Führe eine Scan Aufgabe von der BitDefender Management Konsole aus.
- Mit der Option **Mit BitDefender prüfen** aus dem Windows-Kontextmenü.
- Verwenden Sie BitDefender Manuelle Prüfung um bestimmte Dateien und Ordner direkt zu prüfen.

Führe Scanaufgaben aus

Um Dateien und Ordner auf Malware zu prüfen, befolgen Sie folgende Schritte:

1. Wählen Sie einen Scan Modus unter **Scan Aufgaben** Wählen Sie den Benutzermodus um die Prüfoptionen und die Locations, die geprüft werden sollen, vollständig zu konfigurieren.
2. Wenn Sie eine benutzerdefinierte Prüfung ausgewählt haben, geben Sie das Prüfziel an und konfigurieren Sie die Prüfeinstellungen. Weitere Informationen finden Sie unter „*Konfiguration der On-Demand-Prüfeinstellungen*“ (S. 119).
3. Klicken Sie auf **Prüfung starten** und folgen Sie den Schritten des **BitDefender Scanner**.

Prüfung über Kontextmenü

Dies ist der einfachste und empfohlene Weg eine Datei oder Ordner auf Ihrem Computer zu prüfen. Rechtsklicken Sie das zu prüfende Objekt und wählen Sie **Mit BitDefender prüfen** aus dem Menü aus. Der **BitDefender Scanner** wird erscheinen und Sie durch den Prüfprozess führen.

Weitere Informationen zur Konfiguration der Einstellungen Kontextmenü-Prüfungen finden Sie unter „*Konfiguration der On-Demand-Prüfeinstellungen*“ (S. 119).

Manuelle Prüfung

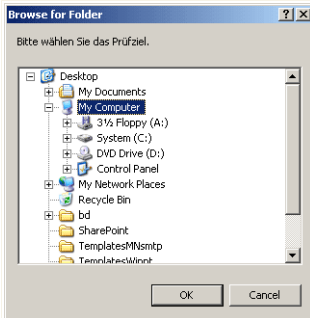
Die Manuelle Prüfung besteht daraus das zu prüfende Objekt direkt über die BitDefender Manuelle Prüfungsoption über den BitDefender Startmenüeintrag zu wählen. Die Scanoptionen sind vor-konfiguriert, um die besten Ergebnisse zu liefern.



Beachten Sie

Die Manuelle Prüfung ist sehr hilfreich, da Sie diese auch im Abgesicherten Modus von Windows verwenden können.

Um das zu prüfende Objekt zu wählen, verwenden Sie den Pfad: **Start** → **Alle Programme** → **BitDefender Business Client** → **BitDefender On-Demand-Prüfung**. Das folgende Fenster wird erscheinen:



Scanziel auswählen

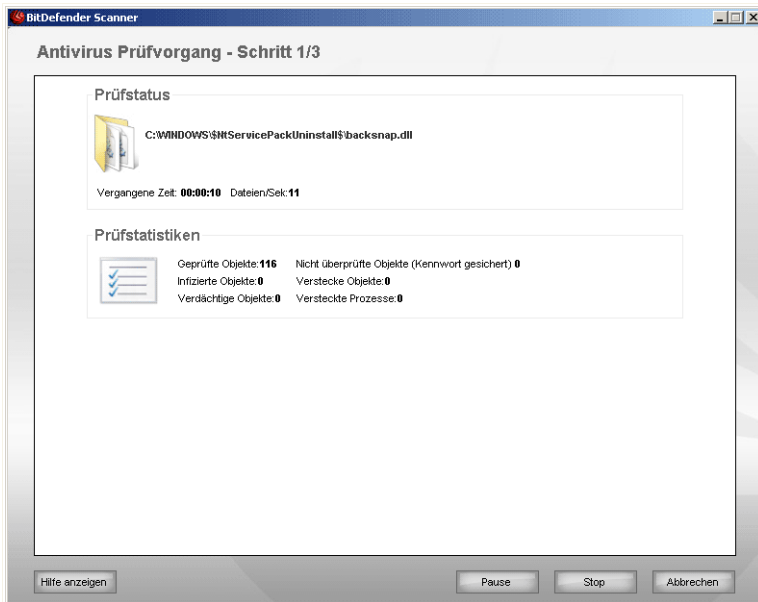
Wählen Sie den Scan Ort und klicken Sie **OK**. Der **BitDefender Scanner** wird erscheinen und Sie durch den Prüfprozess führen.

BitDefender Scanner

Der BitDefender Scanner wird angezeigt, sobald Sie eine On-Demand-Prüfung initiieren. Befolgen Sie die drei Schritt Anleitung um den Prüfvorgang durchzuführen.

Schritt 1/3 - Prüfvorgang

BitDefender prüft die gewählten Dateien und Ordner.



Prüfvorgänge durchführen

Sie können den Vorgangsstatus und die Statistiken hierzu sehen (Prüfgeschwindigkeit, vergangene Zeit, Anzahl der geprüften / infizierten / verdächtigen / versteckten Objekte).



Beachten Sie

Der Prüfvorgang kann, abhängig von der Größe Ihrer Festplatte, einen Moment dauern.

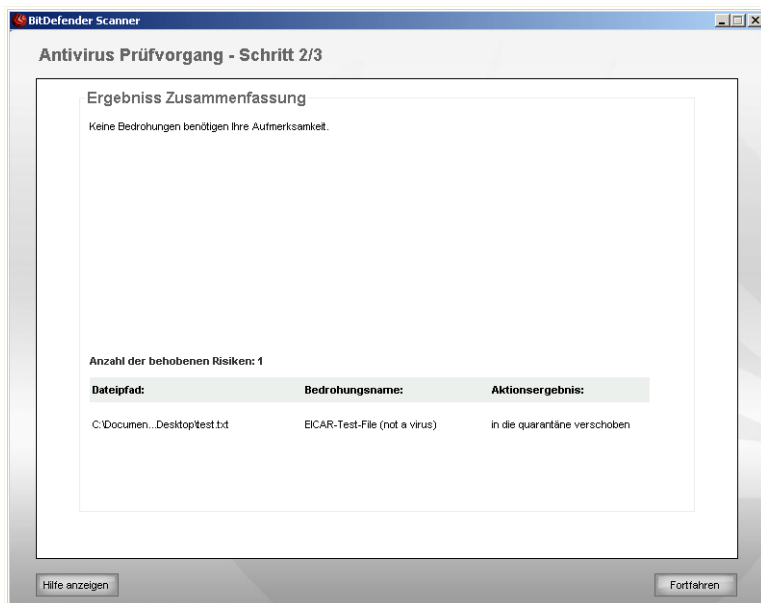
Um den Prüfvorgang vorübergehend zu stoppen klicken Sie einfach auf **Pause**. Um den Prüfvorgang fortzusetzen klicken Sie auf **Fortsetzen**.

Sie können den Prüfvorgang jederzeit durch einen Klick auf **Stop&Ja** abbrechen. Sie gelangen dann direkt zum letzten Schritt des Assistenten.

Bitte warten Sie bis BitDefender den Prüfvorgang beendet hat.

Schritt 2/3 - Aktionsauswahl

Wenn der Prüfvorgang beendet wurde wird Ihnen ein Fenster angezeigt in welchem Sie eine Zusammenfassung angezeigt bekommen.



Aktionen

Sie bekommen die Anzahl der Risiken welche Ihr System betreffen angezeigt.

Die infizierten Objekte werden in Gruppen angezeigt, je nach Malware, mit der sie infiziert sind. Klicken Sie auf den Link, der der Bedrohung entspricht, um weitere Informationen über die infizierten Objekte zu erhalten.

Sie können eine Globale Aktion für jede Gruppe auswählen oder Sie können für jedes Risiko eine eigene Aktion angeben.



Beachten Sie

Sie müssen die Aktion nur manuell auswählen, wenn der BitDefender Scanner als Resultat der Auslösung eines **Manuellen Scans** ist.

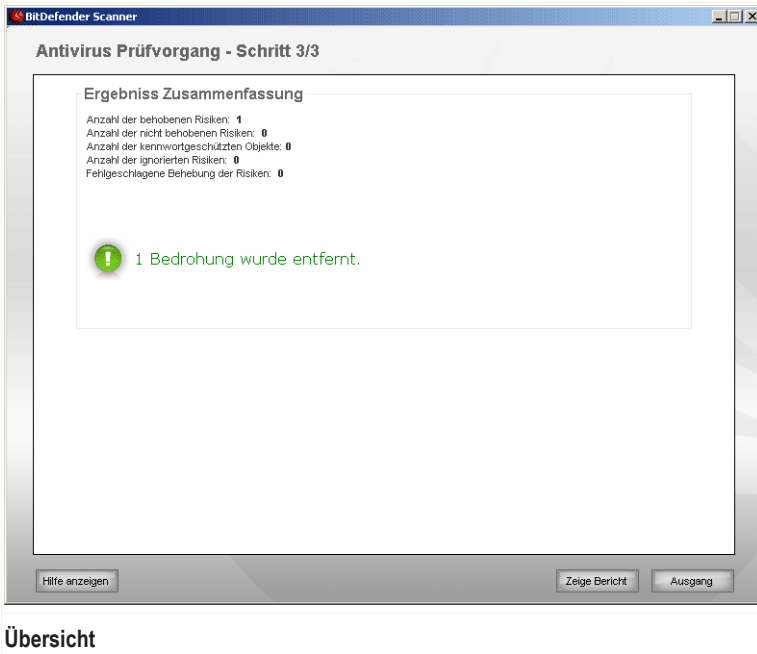
Folgende Aktionen stehen zur Verfügung:

Aktion	Beschreibung
Keine Aktion durchführen	Entdeckte Dateien ignorieren. Sie werden einzig im Prüfbericht protokolliert.
Desinfizieren	Den Malware-Code aus den entdeckten infizierten Dateien entfernen.
Löschen	Infizierte Dateien von der Festplatte entfernen.

Klicken Sie auf **Fortfahren** um die festgelegten Aktionen anzuwenden.

Schritt 3/3 - Zusammenfassung

Wenn BitDefender das Beheben der Risiken beendet hat wird eine Zusammenfassung in einem neuen Fenster geöffnet.



Ihnen wird eine Zusammenfassung angezeigt. Der Bericht wird nun im Bereich **Berichte** angezeigt.



Wichtig

Bitte starten Sie Ihr System neu, wenn Sie dazu aufgefordert werden, damit der Säuberungsprozess abgeschlossen werden kann.

Klicken Sie auf **Beenden**, um das Ergebnisfenster zu schließen.

BitDefender konnte einige Probleme nicht lösen

In den meisten Fällen desinfiziert BitDefender erfolgreich die infizierten Dateien, die er entdeckt hat, oder er isoliert die Infektion. Dennoch gibt es Probleme, die nicht gelöst werden können.

In diesen Fällen empfehlen wir Ihnen unser BitDefender Support Team unter www.bitdefender.de zu kontaktieren. Die Mitarbeiter unseres Supports werden Ihnen dabei helfen die entsprechenden Probleme zu lösen.

Von BitDefender entdeckte Passwortgeschützte Objekte

Die Kategorie der passwortgeschützten Objekte beinhaltet zwei Objektsorten: Archive und Installationsprogramme. Diese stellen keine Bedrohung für das System dar, außer wenn Sie infizierte Dateien enthalten, und wenn diese ausgeführt werden.

Um sicher zu gehen, dass diese Objekte sauber sind:

- Wenn das passwortgeschützte Objekt ein Archiv ist, entpacken Sie die Dateien, die es enthält, um diese einzeln zu prüfen.
- Wenn das passwortgeschützte Objekt ein Installationsprogramm ist, stellen Sie sicher, dass der **Echtzeit-Schutz** aktiviert ist, bevor Sie das Installationsprogramm ausführen. Wenn das Installationsprogramm infiziert ist, so wird BitDefender die Infektion erkennen und isolieren.

Wenn Sie nicht möchten, dass diese Objekte noch einmal von BitDefender entdeckt werden, so müssen Sie sie zu den Ausnahmen des Scan-Prozesses hinzufügen. Wenn Sie Prüfausnahmen hinzufügen möchten, klicken Sie auf **Serverprüfung > Ausnahmen**. Weitere Informationen finden Sie unter „**Prüfausnahmen**“ (S. 129).

Von BitDefender entdeckte verdächtige Dateien

Verdächtige Dateien sind Dateien, die von der heuristischen Analyse als potentiell infiziert erkannt werden, und deren Signaturen noch nicht bekannt sind.

Falls verdächtige Dateien während des Prüfvorganges erkannt werden, werden Sie aufgefordert, diese Dateien zum BitDefender-Labor zu senden. Klicken Sie auf **OK** um diese Dateien zum BitDefender Lab für weitere Analysen zu senden.

9.2.2. Konfiguration der On-Demand-Prüfeinstellungen

Für jeden Prüfmodus können die Aktionen, die für infizierte, verdächtige und verborgene Dateien ausgeführt werden sollen, sowie die Ereignisbenachrichtigungen konfiguriert werden. Wenn Sie das Prüfziel und die Prüfeinstellungen ebenfalls konfigurieren möchten, benutzen Sie den benutzerdefinierten Prüfmodus.

Für die Kontextmenü-Prüfung können die Prüfeinstellungen sowie Aktionen, die für infizierte, verdächtige und verborgene Dateien ausgeführt werden sollen, und die Ereignisbenachrichtigungen konfiguriert werden.



Beachten Sie

Sie können On-Demand-Prüfungen im Bereich **Geplante Aufgaben** planen und konfigurieren. Klicken Sie dazu auf den entsprechenden Link.

So konfigurieren Sie die Einstellungen eines Prüfmodus oder der Kontextmenü-Prüfung:

1. On-Demand-Prüfmodi

Klicken Sie auf den entsprechenden Link **Anpassen**.

Prüfvorgang über Kontextmenü

Klicken Sie auf den Link **Prüfoptionen konfigurieren**.

Das Konfigurationsfenster wird erscheinen.

2. Klicken sie auf die Tabs und konfigurieren Sie die entsprechenden Einstellungen wie gewünscht.
3. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.

Das Konfigurationsfenster hat zwei Tabs:

Tab	Beschreibung
Prüfeinstellungen	In diesem Tab können sie die Prüfeinstellungen und das Prüfziel konfigurieren. Sie können BitDefender so einstellen, dass nur Dateien mit bestimmten Endungen geprüft werden oder das bestimmte Dateiformate, Archive oder Dateien, die eine bestimmte Größe überschreiten von der Prüfung ausgelassen werden.
Aktionen	In diesem Tab können Sie die Aktionen konfigurieren, die durchgeführt werden sollen wenn BitDefender infizierte, verdächtige und verborgene Dateien entdeckt.
Benachrichtigungen	In diesem Tab können Sie die Benachrichtigungsoptionen für die On-Demand-Prüfung einstellen.

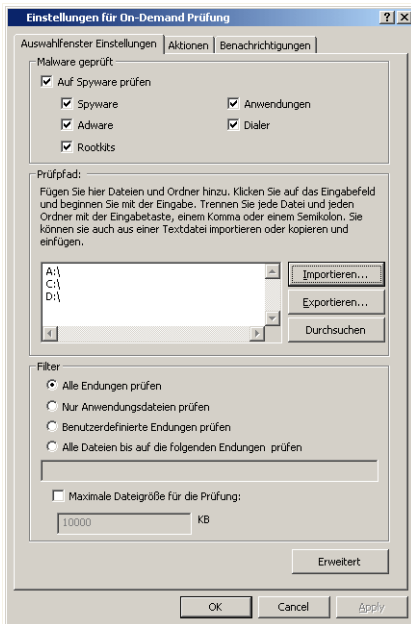
Tab Prüfeinstellungen

In diesem Tab können sie die Prüfeinstellungen und das Prüfziel konfigurieren.



Beachten Sie

Die Prüfeinstellungen können nur für den benutzerdefinierten Prüfmodus und die Prüfung über Kontextmenü eingestellt werden.



Tab Prüfeinstellungen

Spezielle Malware von der Prüfung ausschließen

Sie können BitDefender so einstellen, dass neben den Virensignaturen auch die Signaturen folgender Bedrohungen verwendet werden:

- Spyware
- Adware
- Anwendungen
- Dialers
- Rootkits

Lassen sie zu diesem Zweck die Kontrollkästchen zu **Auf Riskware prüfen** und zu den spezifischen Malware-Bedrohungen, auf die geprüft werden soll, markiert.



Wichtig

Alle erkannte Malware wird als infiziert behandelt.

Wenn Sie möchten, dass BitDefender nur Virensignaturen für die Prüfung auf Basis von Signaturen verwendet, so lassen Sie das Kontrollkästchen zu **Auf Riskware prüfen** frei.

Festlegen der Zielobjekte



Beachten Sie

Kann nicht über Kontextmenü geprüft werden.

Befolgen Sie eine der folgenden Möglichkeiten, um spezielle Objekte (Laufwerke, Dateien, Ordner) festzulegen, die geprüft werden sollen:

- Geben Sie in das Editierfeld den vollständigen Pfad der zu prüfenden Objekte ein, wobei Sie diese mit der Eingabetaste, einem Komma oder Strichpunkt trennen müssen.
- Klicken Sie auf **Durchsuchen** und wählen Sie die zu prüfenden Objekte.
- Wenn Sie über eine Textdatei verfügen, die eine Liste der Locations (von Dateien und Ordnern) enthält, die geprüft werden sollen, klicken Sie auf **Importieren** und laden Sie die entsprechende Datei. Sie können die Locations auch aus der Textdatei kopieren und direkt in das Editierfeld einfügen.

Um die Liste der Dateien und Ordner als eine Textdatei zu speichern, klicken Sie auf **Exportieren**.

Dateien anhand der Endungen prüfen

Bestimmte Dateisorten sind anfälliger auf Viren als andere. So ist zum Beispiel das Risiko beim Ausführen einer `.exe` Datei höher, als beim Öffnen einer `.txt` oder einer `.gif` Datei.

Um festzulegen welche Dateisorten geprüft werden sollen, wählen Sie zwischen den folgenden Optionen wählen:

Optionen	Beschreibung
Alle Endungen prüfen	Prüft alle vorhandenen Dateien.
Nur Anwendungsdateien prüfen	Nur Anwendungsdateien werden geprüft. Diese Kategorie ist auf Dateien mit den folgenden Erweiterungen beschränkt: 386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; lacddb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp;

Optionen	Beschreibung
	mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsn; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp Viren werden normalerweise über Anwendungsdateien übertragen. Deshalb sollten diese Dateien immer überprüft werden.
Benutzerdefinierte Endungen prüfen	Nur Dateien mit den festgelegten Endungen werden geprüft. Sie müssen in das Editierfeld die Dateieendungen eingeben, die von BitDefender geprüft werden sollen, wobei diese mit Strichpunkten (",") zu trennen sind.
Alle bis auf die folgenden Endungen prüfen	Die Dateien mit den festgelegten Endungen werden NICHT geprüft. Sie müssen in das Editierfeld die Dateieendungen eingeben, die NICHT von BitDefender geprüft werden sollen, wobei diese mit Strichpunkten (",") zu trennen sind. Sie sollten Dateierarten, die bekannt für Vren sind nicht von der Prüfung ausschließen, wie beispielsweise .exe, .doc, .ppt, .xls, .rtf, .pif, .bat und Andere.

Dateien anhand der Größe prüfen.

Die Prüfung großer Dateien erfordert zusätzliche Systemressourcen, was das System verlangsamt.

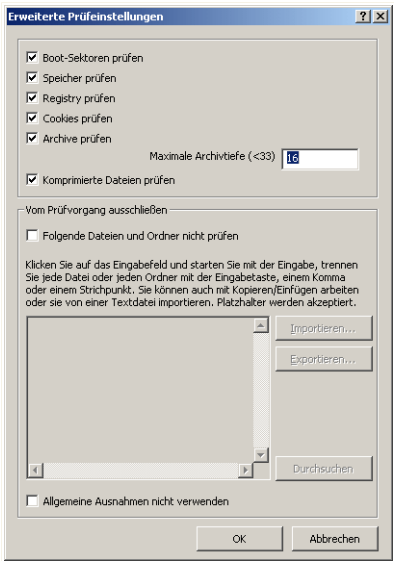
Legen Sie das Größenlimit (in KB) der zu prüfenden Dateien in dem Feld **Maximale Größe von zu prüfenden Dateien** fest. Wenn Sie beispielsweise 2000 eingeben, werden alle Dateien die größer als 2000 KB sind von der Prüfung ausgeschlossen.

Wenn Sie möchten, dass alle Dateien, unabhängig von deren Größe geprüft werden, befolgen Sie eine der folgenden Möglichkeiten:

- Lassen Sie das Kontrollkästchen zu **Maximale Größe von zu prüfenden Dateien** frei.
- Geben Sie als Größenbegrenzung 0 KB ein.

Weitere Einstellungen und Ausnahmen konfigurieren

Um weitere Einstellungen oder Ausnahmen der On-Demand Prüfung vorzunehmen, klicken Sie auf **Erweitert**. Ein neues Konfigurationsfenster wird sich öffnen.



Mehr Einstellungen

Folgende erweiterte Prüfeinstellungen können konfiguriert werden:

Optionen	Beschreibung
Boot-Sektoren	Den Bootsektor der verfügbaren Laufwerke prüfen.
Speicher prüfen	Den Systemspeicher prüfen.
Registry prüfen	Die Windows-Registry prüfen.
Cookies prüfen	Cookie-Dateien prüfen.
Archive prüfen	Archivierte Dateien prüfen. Sie können eine maximale Archivtiefe festlegen, um Dateien zu prüfen, die mehrfach archiviert wurden. Wenn Sie Dateien prüfen wollen, egal wie häufig diese archiviert wurden, stellen Sie die maximale Archivtiefe auf 0 ein. Wenn Sie diese Option wählen, wird die Leistung des Systems verlangsamt und die Prüfzeit verlängert.
Komprimierte Dateien prüfen	Komprimierte Dateien prüfen.

Um Dateien und Ordner von der On-Demand-Prüfung auszuschließen:

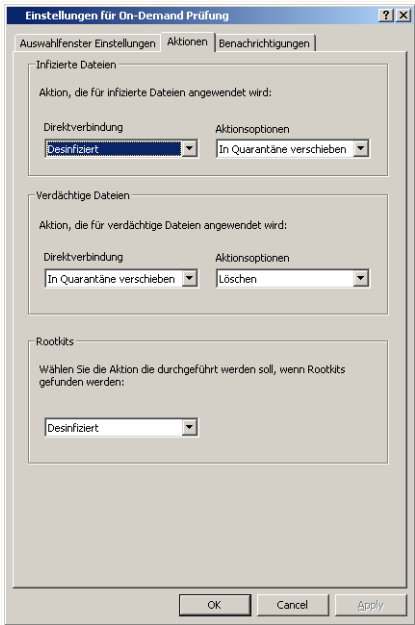
1. Wählen Sie **Folgende Dateien und Ordner nicht prüfen**.
2. Wählen Sie eine der folgenden Methoden:
 - Geben Sie in das Editierfeld den vollständigen Pfad der Dateien und Ordner ein, die nicht geprüft werden sollen, wobei Sie diese mit der Eingabetaste, einem Komma oder Strichpunkt trennen müssen.
 - Klicken Sie auf **Durchsuchen** und wählen Sie die Dateien und Ordner, die nicht geprüft werden sollen.
 - Wenn Sie über eine Textdatei verfügen, die eine Liste der Locations (von Dateien und Ordnern) enthält, die nicht geprüft werden sollen, klicken Sie auf **Importieren** und laden Sie die entsprechende Datei. Sie können die Locations auch aus der Textdatei kopieren und direkt in das Editierfeld einfügen.

Um die Liste der Dateien und Ordner als eine Textdatei zu speichern, klicken Sie auf **Exportieren**. Auf diese Weise können Sie diese Liste auf andere File Server laden, um die Prüfausnahmen zu konfigurieren.

Standardmäßig gelten die im Abschnitt **Ausnahmen** definierten allgemeinen Ausnahmen für die On-Demand-Prüfung. Sie können festlegen, dass die Ausnahmen für den aktuellen Moduls nicht gelten.

Tab Aktionen

In diesem Tab können Sie die Aktionen konfigurieren, die durchgeführt werden sollen wenn BitDefender infizierte, verdächtige und verborgene Dateien entdeckt.



Tab Aktionen

Sie können verschiedene Aktionen für jede Art der entdeckten Datei auswählen: infiziert, verdächtig oder Rootkit. Wählen Sie die durchzuführende Aktion für die erkannten Dateien aus den entsprechenden Menüs.



Beachten Sie

Sie können zwei Aktionen für Dateien konfigurieren, die infiziert oder verdächtig sind. Die zweite Aktion wird durchgeführt falls die Erste fehlschlägt.

Aktionen für infizierte Dateien. Folgende Aktionen stehen für infizierte Dateien zur Verfügung:

Aktion	Beschreibung
Desinfizieren	Den Malware-Code aus den entdeckten infizierten Dateien entfernen. Die Wiederherstellung kann in einigen Fällen fehlschlagen (wenn die Datei z. B. innerhalb eines bestimmten Archivs ist oder sie von einem laufenden Prozess verwendet wird).
In Quarantäne verschieben	Infizierte Dateien von Ihrer ursprünglichen Position in den Quarantäne-Ordner verschieben. Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht kein Infektionsrisiko?

Aktion	Beschreibung
Löschen	Infizierte Dateien direkt und ohne Warnung von der Festplatte entfernen.
Ignorieren	Nur die entdeckten infizierten Dateien im Prüfbericht protokollieren. Um den Prüfbericht zu sehen, klicken Sie auf Berichte im Baumannu wenn die Prüfung beendet wurde.

Aktionen für verdächtige Dateien. Folgende Aktionen stehen für verdächtige Dateien zur Verfügung:

Aktion	Beschreibung
In Quarantäne verschieben	Infizierte Dateien von Ihrer ursprünglichen Position in den Quarantäne-Ordner verschieben. Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht kein Infektionsrisiko?
Löschen	Verdächtige Dateien direkt und ohne Warnung von der Festplatte entfernen.
Ignorieren	Nur die entdeckten verdächtigen Dateien im Prüfbericht protokollieren. Um den Prüfbericht zu sehen, klicken Sie auf Berichte im Baumannu wenn die Prüfung beendet wurde.

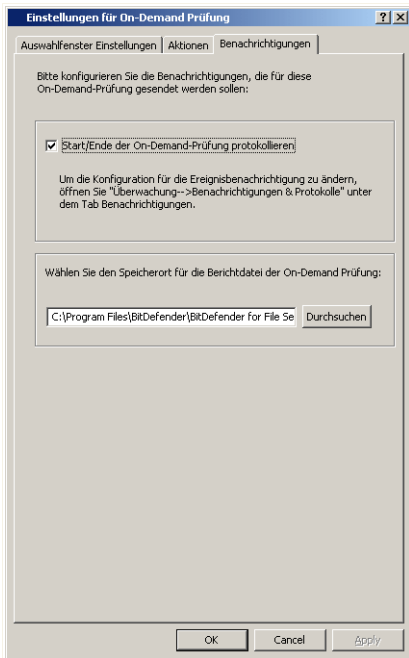
Wenn Sie möchten, dass BitDefender verdächtige Dateien automatisch zum BitDefender Labor für weitere Analysen sendet, wählen Sie das entsprechende Kontrollkästchen.

Aktionen für Rootkits (verborgene Objekte). Folgende Aktionen stehen für Rootkits zur Verfügung:

Aktion	Beschreibung
Desinfizieren	Den Malware-Code aus den entdeckten infizierten Dateien entfernen. Die Wiederherstellung kann in einigen Fällen fehlschlagen (wenn die Datei z. B. innerhalb eines bestimmten Archivs ist oder sie von einem laufenden Prozess verwendet wird).
Ignorieren	Nur die entdeckten Rootkits im Prüfbericht protokollieren. Um den Prüfbericht zu sehen, klicken Sie auf Berichte im Baumannu wenn die Prüfung beendet wurde.

Tab Benachrichtigungen

BitDefender kann so eingestellt werden, dass Sie über bestimmte Ereignisse während des Betriebs benachrichtigt werden. In diesem Tab können Sie die Benachrichtigungsoptionen für die On-Demand-Prüfung einstellen.



Tab Benachrichtigungen

Wählen Sie **Start/Ende der On-Demand Prüfung protokollieren**, um den Start und das Ende der Prüfung in der Bitdefender Protokolldatei aufzuzeichnen. Wenn Sie möchten, dass BitDefender Mail- oder Net Send Benachrichtigungen zu bestimmten Personen sendet, öffnen Sie **Benachrichtigungen & Protokolle**, den Tab **Benachrichtigungen** und konfigurieren Sie das Ereignis **On-Demand Prüfung entsprechend**. Weitere Informationen finden Sie hier: „*Ereignisbenachrichtigung konfigurieren*“ (S. 53).

Ein detaillierter Prüfbericht wird jedes Mal erstellt, wenn Sie eine On-Demand-Prüfung durchführen. Der Bericht wird im XML-Format erstellt und kann mithilfe eines Browsers betrachtet werden. Um einen Bericht zu betrachten, öffnen Sie **Berichte**.

Standardmäßig werden die Berichte der On-Demand-Prüfung im Ordner `C:\Programmdateien\BitDefender\BitDefender Security for File Server\Berichte` gespeichert. Falls Sie einen anderen Speicherort wählen möchten, klicken Sie auf **Durchsuchen** und wählen Sie den Ordner in dem die Berichte gespeichert werden sollen.

9.3. Prüfausnahmen

Gemäß den Microsoft Empfehlungen schließt die BitDefender Sicherheit for File Server automatisch davon aus, mehrere Dateien, Ordner und Prozesse zu scannen, die oder verwendet durch die Microsoft Server Produkte gehören:

- Microsoft Exchange 2007 / 2003 / 2000 / 5.5
- Microsoft ISA Server 2006 / 2004 / 2000
- Microsoft SharePoint 2003

Ähnlich scannt die BitDefender Security for File Server spezifische Positionen und Prozesse bezogen auf BitDefender Security for Windows Servers und BitDefender Management Server nicht, um zu vermeiden, ihre Operation zu stören und ihre Leistung zu verbessern.

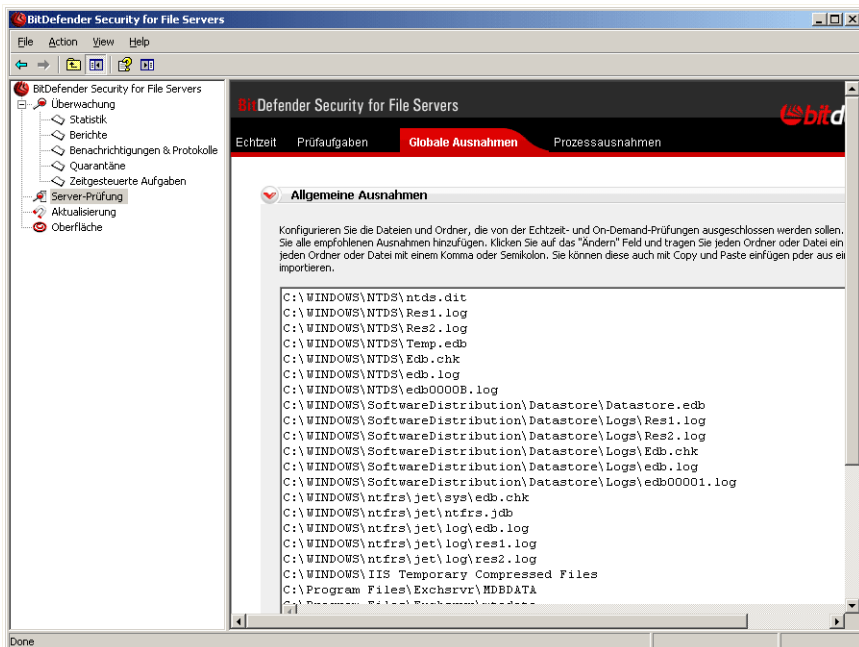
Der Ausschluss-Prozess kommt während der Installation vor. Sie können die vom Scanvorgang ausgeschlossenen Positionen und Prozesse unter dem Tab **Globale Ausnahmen** bzw. **Prozesse Ausnahmen** Später, wenn Sie Microsoft Server Produkte oder BitDefender Sicherheitslösungen hinzufügen bzw. entfernen, können Sie zu diese Tabs gehen und aktualisieren Sie den Update automatisch.

Sie können andere Dateien, Ordner und Prozesse manuell vom Scan ausschließen. Beispielsweise können Sie einen Backupprozess ausschließen, um Einmischung zu vermeiden und es zu beschleunigen. Sie können wahlweise auch gegenwärtige Ausnahmen entfernen.

Innerhalb der automatischen Ausnahmen, werden Sie spezifische Elemente manuell ausschließen müssen. Weitere Informationen finden Sie unter „*Manuell auszuschließende Elemente*“ (S. 132).

9.3.1. Globale Ausnahmen

Um von Echtzeit-Scan und On-Demand Scan ausgeschlossenen Dateien und Ordner zu konfigurieren, klicken Sie im Baummenü auf **Serverprüfung** und dann auf den Tab **globale Ausnahmen**.



Prüfausnahmen

Die Dateien und Ordner die sowohl von der Prüfung in Echtzeit als auch von der On-Demand-Prüfung ausgeschlossen sind, sind in dem Feld aufgelistet.

Befolgen Sie eine der folgenden Möglichkeiten, um Dateien und Ordner von der Prüfung auszuschließen:

- ☐ Geben Sie in das Editierfeld den vollständigen Pfad der Dateien und Ordner ein, die nicht geprüft werden sollen, wobei Sie diese mit der Eingabetaste, einem Komma oder Strichpunkt trennen müssen.
- ☐ Klicken Sie auf **Durchsuchen** und wählen Sie die Dateien und Ordner, die nicht geprüft werden sollen.
- ☐ Wenn Sie über eine Textdatei verfügen, die eine Liste der Locations (von Dateien und Ordnern) enthält, die nicht geprüft werden sollen, klicken Sie auf **Liste importieren** und laden Sie die entsprechende Datei. Sie können die Locations auch aus der Textdatei kopieren und direkt in das Editierfeld einfügen.

Um die Liste der Dateien und Ordner als eine Textdatei zu speichern, klicken Sie auf **Liste exportieren**. Auf diese Weise können Sie diese Liste auf andere File Server laden, um die Prüfausnahmen zu konfigurieren.

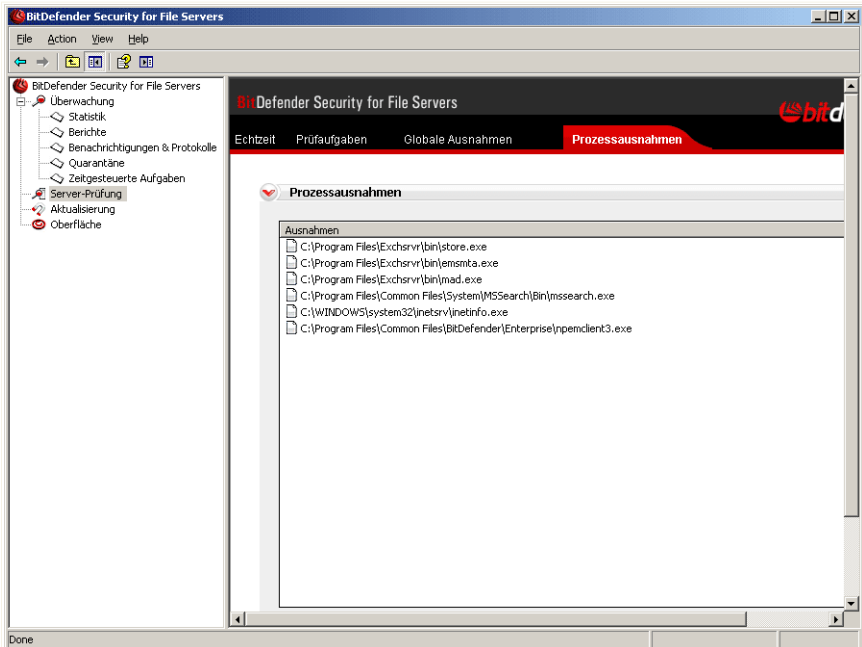
Klicken Sie auf **Update Ausnahmen** um automatisch nach ausgeschlossenen Dateien und Ordner, das Microsoft oder Bitdefender empfehlen nicht gescannt zu werden, zu

suchen. Sie sollten Ausnahmen aktualisieren, wenn Sie sie zufällig entfernt haben, und wenn Sie ein neues Server-Produkt von Microsoft oder BitDefender Sicherheitslösung installieren.

Klicken Sie auf **Anwenden**, um die Änderungen zu speichern.

9.3.2. Prozessausnahmen

Um den Echtzeitschutz zu konfigurieren, klicken Sie auf **Serverprüfung** im Baummenu und dann auf den Tab **Prozessausnahmen**.

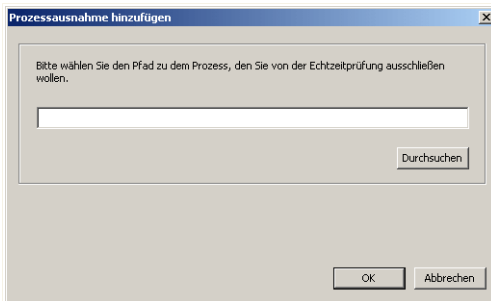


Prüfausnahmen

Das erste Mal, wenn Sie auf diese Abteilung zugreifen, können Sie die automatisch von der Echtzeitabtastung ausgeschlossenen Prozesse, wie empfohlen durch Microsoft oder BitDefender, sehen. Sie können neue neue Anwendungen zu Liste hinzufügen oder gegenwärtige Anwendungen entfernen.

Um einen bestimmten Prozess vom Echtzeitscan auszuschließen, folgen Sie diesen Schritten:

1. Klicken Sie auf **Hinzufügen**. Ein neues Fenster wird sich öffnen.



Anwendungen hinzufügen

2. Klicken Sie auf **Durchsuchen** und wählen Sie das Programm.
3. Klicken Sie auf **OK** um die Regel zur Liste hinzuzufügen.

Um eine Ausnahme in der Liste zu bearbeiten, wählen Sie diese aus oder doppelklicken Sie darauf und klicken Sie dann auf **Ändern**. Um eine vom Echtzeitscan ausgeschlossene Anwendung zu entfernen, markieren Sie diese und klicken Sie dann auf **Entfernen**.

Wählen Sie **Update Ausnahmen** um automatisch Anwendungen auszuschließen, dass Microsoft oder BitDefender empfehlen, in der Echtzeit nicht gescannt zu werden. Sie sollten Ausnahmen aktualisieren, wenn Sie sie zufällig entfernt haben, und wenn Sie ein neues Server-Produkt von Microsoft oder BitDefender Sicherheitslösung installieren.

9.3.3. Manuell auszuschließende Elemente

Je nachdem, welche Anwendungen auf dem Server laufen und welche Ausnahmen für sie empfohlen werden, müssen Sie eventuell zusätzliche Ausnahmen manuell hinzufügen.

Zum Beispiel:

1. Wenn ein Mailserver ausser Exchange Server auf der Maschine läuft, müssen die folgenden Positionen ausgeschlossen werden:
 - der Ordner, in dem der Mail-Server installiert ist.
 - der Ordner, in dem die Postfächer und Mail-Warteschlangen abgelegt sind.
2. Wenn Exchange Server 2003 auf der Maschine läuft:
 - a. Wenn Sie den Microsoft BackOffice POP3 Connector verwenden, um E-Mails von einem externen POP3-Benutzerkonto zu erhalten, schließen Sie den Ordner für eingehende Mails aus. Die standard-Location lautet:

```
%ProgramFiles%\Microsoft      Windows      Small      Business  
Server\Networking\POP3\Incoming Mail\
```

- b. Schließen Sie den Ordner für die Komprimierung von Internet Information Services (IIS) 6.0 aus, der mit Outlook Web Access 2003 verwendet wird. Die Standard Position lautet:

`%SystemRoot%\IIS Temporary Compressed Files\`

- c. Wenn Cluster verwendet werden, schließen Sie die folgenden Dateien aus:

- Quorum disk
- `%Winnt%\Cluster folder\`
- `\Exchsrvr\Conndata folder\`

`%SystemRoot%` und `%ProgramFiles%` sind Systemvariablen die von dem Betriebssystem und der Computerkonfiguration abhängen. Sie können mit dem Befehl SET bestimmt werden.



Beachten Sie

Eine aktualisierte Liste der von Microsoft empfohlenen Ausnahmen finden Sie unter [article](#).

9.4. AntiViren-Schutz Prüfung

Um zu überprüfen ob BitDefender Antivirus funktionstüchtig ist können sie eine spezielle Test-Datei verwenden: *EICAR Standard Anti-virus Test*. EICAR steht für *European Institute of Computer Anti-virus Research*. Dies ist eine Test-Datei die von Antivirus-Produkten entdeckt wird.

Die Datei kann mit einem Texteditor erstellt werden, vorausgesetzt die Datei wird im Standard MS-DOS-ASCII-Format gespeichert und hat eine Länge von 68 Bytes. Sie könnte auch ein Größe von 70 Byte haben, wenn der Editor an das Dateieinde ein CR/LF (Carriage Return/Linefeed) setzt.

Die Datei muss den folgenden Einzeiler enthalten :

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

Kopieren Sie diese Zeile und speichern Sie die Datei unter irgendeinem Namen mit der Endung `.COM`, beispielsweise `EICAR.COM`. BitDefender sollte diese Datei als infiziert behandeln.

Es besteht kein Grund zur Sorge, da es sich nicht um einen echten Virus handelt. `EICAR.COM` gibt bei der Ausführung lediglich folgenden Text aus: `EICAR-STANDARD-ANTIVIRUS-TEST-FILE` und beendet die Anwendung.



Beachten Sie

Die Datei wurde jedoch aus einem einfachen Grund nicht in das Paket eingefügt: es sollten bei Anwendern, die BitDefender oder andere Virens Scanner nutzen, falsche Alarme vermieden werden. Sie können `EICAR.COM` an einem sicheren Ort aufbewahren und den Serverschutz von Zeit zu Zeit testen.

Sie können die Webseite von EICAR unter <http://eicar.com> besuchen, die Beschreibung lesen und die Datei von einer der Locations der folgenden Webseite herunterladen: http://eicar.com/anti_virus_test_file.htm.

10. Aktualisierung

Jeden Tag werden neue Viren und Spyware entdeckt und identifiziert. Aus diesem Grund ist es von großer Bedeutung, dass Sie BitDefender stets mit den neuesten Virensignaturen versorgen.

Mit der Funktion des automatischen Updates kann BitDefender automatisch und regelmäßig aktualisiert werden, ohne dass der Administrator hierfür eingreifen müsste. Standardmäßig prüft BitDefender stündlich auf vorhandene Updates. Wenn neue Malware-Signaturen oder eine Engine entdeckt werden, wird Bitdefender diese automatisch herunterladen und installieren. Um die Häufigkeit der Updates zu ändern, öffnen Sie den Tab **Einstellungen**.

Das automatische Update kann jederzeit durchgeführt werden, indem Sie auf **Jetzt aktualisieren** im Bereich **Update** klicken oder indem Sie eine **Geplante Update-Aufgabe** erstellen.



Beachten Sie

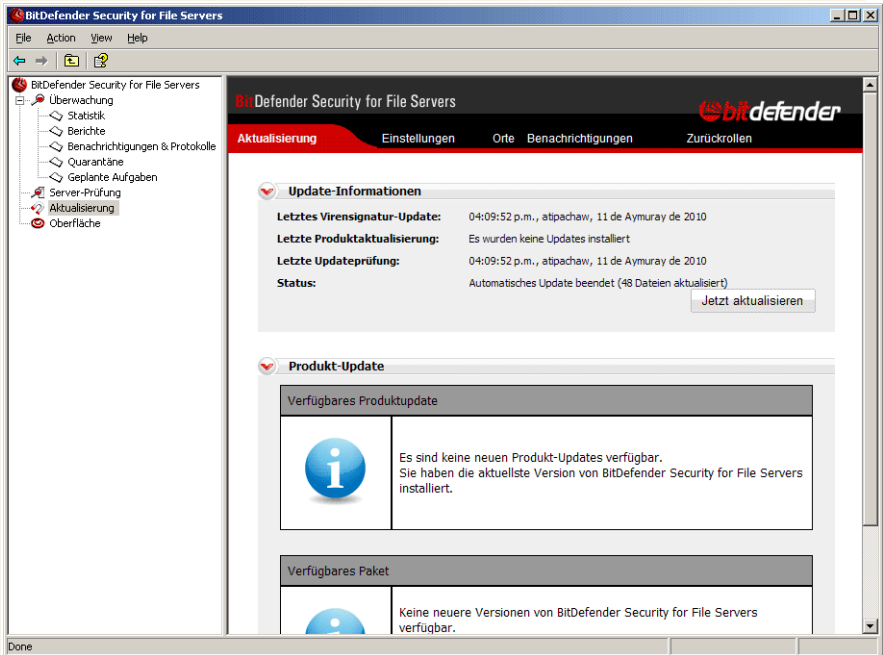
Um den Betrieb des Servers nicht zu behindern, werden die Produkt-Updates nicht automatisch installiert. Öffnen Sie den Bereich **Update** regelmäßig, um zu sehen ob Produkt-Updates verfügbar sind und um diese zu installieren.

Die Updates können folgendermaßen unterteilt werden:

- **Antivirus-Updates** - neue Virus- und Spyware-Signaturen sowie die Engines werden aktualisiert, um einen aktuellen Schutz zu gewährleisten.
- **Product updates** - wenn eine neue Version auf dem Markt erscheint, enthält diese zur Leistungssteigerung des Produkts neue Funktionen und Scantechniken.

10.1. Aktualisierung

Um Informationen über den Update-Status zu erhalten und um zu sehen ob neue Updates verfügbar sind, klicken Sie auf **Update** im Baummenu und dann auf den Tab **Update**.



Aktualisierung

Wenn Sie den BitDefender sofort aktualisieren möchten, klicken Sie auf **Jetzt aktualisieren**. Das Update-Modul wird bei den festgelegten Locations nach Updates suchen. Wenn neue Malware-Signaturen oder eine Engine entdeckt werden, wird Bitdefender diese automatisch herunterladen und installieren.

10.1.1. Update-Informationen

In dem Feld **Update-Informationen** können Sie den Update-Status sehen, wann die letzte Prüfung auf Updates und wann das letzte Update durchgeführt wurde.

10.1.2. Produkt-Update

Die Produktupdates unterscheiden sich von den Signatur Updates. Ihre Funktion ist die Lieferung neuer Bug-Fixes und Funktionen für das Produkt.

Es gibt zwei Arten von Updates für das Produkt:

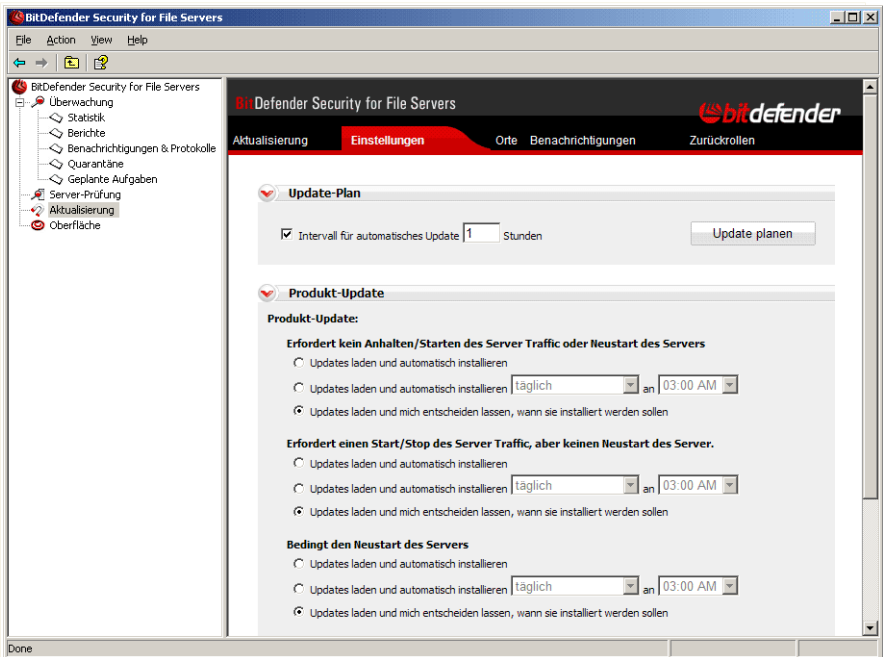
- **Produkt-Updates** - dies sind kumulative EXE-Dateien, die alle Dateien beinhalten, die seit der ersten Veröffentlichung des Produktes geändert wurden.
- **Version-Updates** - dies sind Installationspakete (Kits) mit einer neu veröffentlichten Version des Produktes.

Sobald Produkt-Updates verfügbar sind oder eine neuere Version erhältlich ist, wird hier die entsprechende Information angezeigt.

Standardmäßig werden Produkt-Updates und Version-Updates nicht automatisch installiert, da dies einen Neustart des Systems erfordern oder den Server-Datenverkehr unterbrechen könnte. Es wird empfohlen, die neuesten Updates so bald wie möglich zu installieren. Weitere Informationen zur Aktivierung und Konfiguration von automatischen Produkt-Updates finden Sie unter: „*Konfiguriere Produkt Updates*“ (S. 139).

10.2. Update-Einstellungen

Klicken Sie auf **Update** im Baummenu und dann auf den Tab **Einstellungen** um die Häufigkeit und die Einstellungen der Updates zu konfigurieren.



Update-Einstellungen

10.2.1. Update-Planung konfigurieren

Es gibt zwei Möglichkeiten BitDefender Security for File Server regelmäßig zu aktualisieren:

- **Verwendung des automatischen Updates.** Mit der Funktion des automatischen Updates kann BitDefender automatisch und regelmäßig aktualisiert werden, ohne dass der Administrator hierfür eingreifen müsste. Standardmäßig prüft BitDefender stündlich auf vorhandene Updates bei den festgelegten Update-Locations. Wenn neue Malware-Signaturen oder eine Engine entdeckt werden, wird Bitdefender diese automatisch herunterladen und installieren.



Wichtig

Lassen Sie das automatische Update aktiviert um gegen die aktuellsten Bedrohungen geschützt zu sein.

Um einzustellen, wie häufig BitDefender eine Prüfung auf Updates durchführt, befolgen Sie diese Schritte:

1. Geben Sie die Anzahl der Stunden zwischen zwei aufeinander folgenden Updateprüfungen in das Feld **Zeitintervall für automatisches Update** ein.
2. Klicken Sie auf **Anwenden**, um die Änderungen zu speichern.

Um das automatische Update zu deaktivieren, befolgen Sie diese Schritte:

1. Deaktivieren Sie das Kontrollkästchen **Zeitintervall für automatisches Update**.
 2. Klicken Sie auf **Anwenden**, um die Änderungen zu speichern.
- **Eine geplante Update-Aufgabe verwenden.** Mit geplanten Update-Aufgaben können die Malware-Signaturen und die Engines entsprechend eines eingestellten Zeitplans aktualisiert werden. Klicken Sie auf **Update planen**, um eine geplante Update-Aufgabe zu erstellen. Weitere Informationen finden Sie unter „Update-Aufgaben“ (S. 83).



Beachten Sie

Die geplanten Update-Aufgaben haben keinen Einfluss auf das automatische Update-Modul. Es führt weiterhin die regelmäßigen Überprüfungen der Update-Locations auf neue Signaturen durch.

10.2.2. Konfiguriere Produkt Updates

Produkt Updates regelmäßig zu installieren, ist für die Sicherheit Ihres Servers sehr wichtig. Abhängig von dem Grad der Beeinträchtigung des Servers, gibt es drei Arten von Produkt Updates:

- Produkt Updates, die kein anhalten des Server Verkehrs oder Neustart des Servers verlangen
- Produkt Updates, die ein Anhalten des Server Verkehrs verlangen, aber keinen Neustart des Servers
- Produkt Updates, die einen Neustart des Server verlangen

Um automatische Downloads und Installation für jede Art von Produkt Updates zu konfigurieren, wählen Sie eine der folgenden Optionen:

Updates laden und automatisch installieren

Wählen Sie diese Option und BitDefender wird automatisch Produkt Updates laden und installieren. Dies ist die empfohlene Wahl für Produkt Updates, die kein Anhalten des Server Verkehrs oder Neustart des Servers verlangen.

Updates automatisch laden und installieren... in...

Wählen Sie diese Option, wenn sie wollen, dass BitDefender verfügbare Updates zu einer gewissen Zeit installiert. Wählen Sie aus der Liste das Datum (Tag und Zeit) wann dies geschehen soll.

Auf diese Weise können Sie BitDefender konfigurieren Produkt Updates an Zeiten durchzuführen, zu denen die wenigsten Störungen der Server Aktivität zu erwarten sind (nachts bspw.)

Lade Updates und lasse mich entscheiden, wann diese installiert werden

Wählen Sie diese Option, wenn Sie wollen, dass BitDefender automatisch Produkt Updates lädt, sie aber entscheiden, wann sie installiert werden sollen. Dies ist die empfohlene Auswahl für Produkt Updates, die ein Anhalten des Server Verkehrs und einen Neustart des Servers verlangen.

Um die automatischen Produkt Updates zu deaktivieren, wählen Sie **Keine automatischen Produkt Updates**.



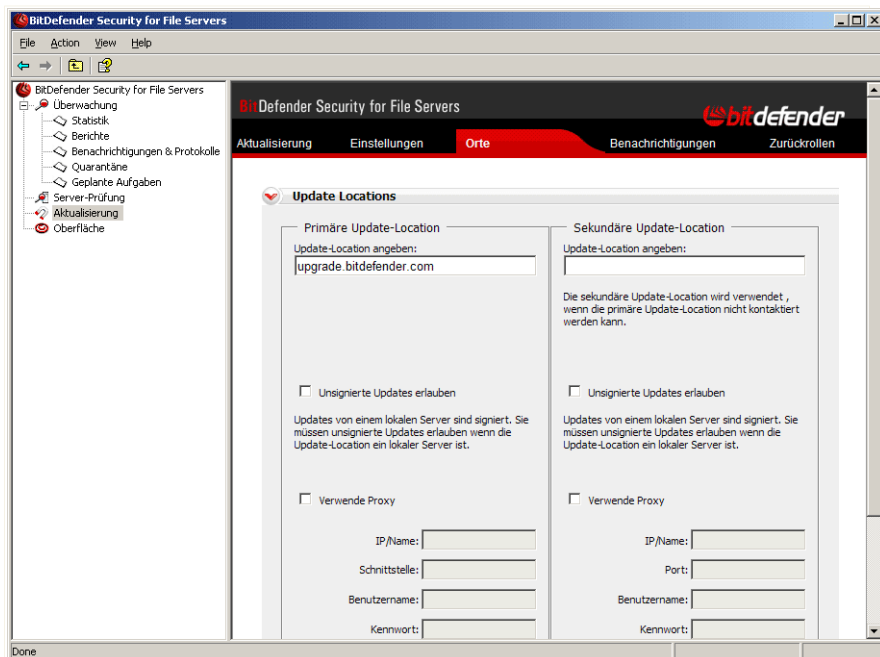
Beachten Sie

Ihr Server wird gefährdet sein, wenn Sie nicht regelmässig Updates installieren.

Klicken Sie auf **Anwenden**, um die Änderungen zu speichern.

10.3. Update Locations

Um die Update Orte festzulegen, klicken Sie **Update** im Baum Menu und dann **Orte**.



Update Locations

Die Updates können im lokalen Netzwerk, über das Internet, direkt oder über einen Proxy-Server durchgeführt werden.

Für zuverlässigere und schnellere Update können zwei Update-Locations angegeben werden: Eine **Erste Update-Location** und eine **Zweite Update-Location**. Die folgenden Optionen müssen für beide konfiguriert werden:

- **Update-Location** - geben Sie die Adresse des Update-Servers an. Standardmäßig lautet die erste Update-Location: `upgrade.bitdefender.com`.

Wenn in Ihrem Netzwerk mehrere BitDefender-Produkte installiert sind, können Sie einen lokalen Server als primäre Update-Location und `upgrade.bitdefender.com` als sekundäre festlegen; die sekundäre wird verwendet, falls die primäre nicht erreichbar ist. So können Sie den Internet-Datenverkehr während der Aktualisierung reduzieren.



Beachten Sie

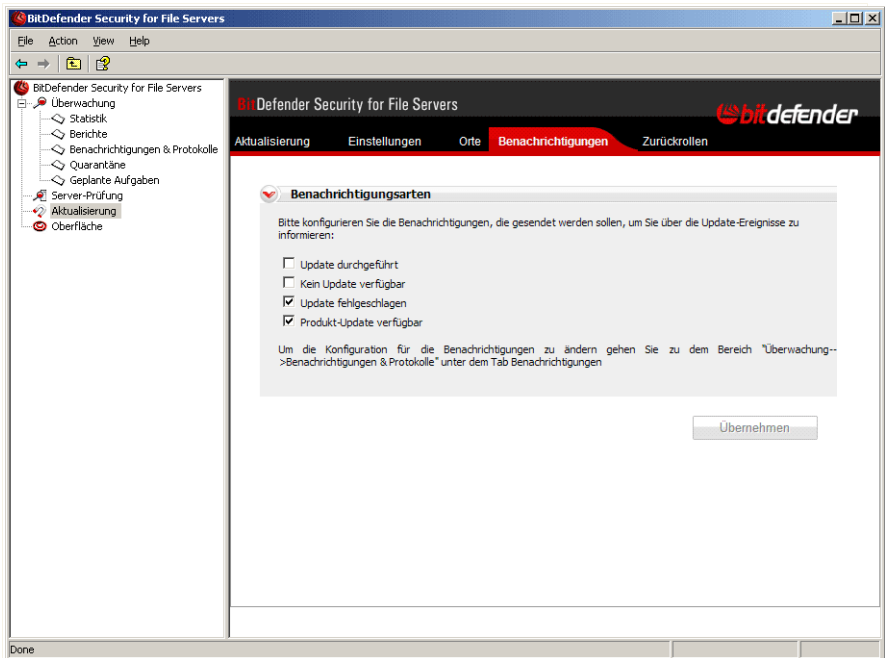
Die lokale Update-Location kann mit BitDefender Update Server (ein Teil von BitDefender Management Server) eingerichtet werden oder mithilfe eines Web-Servers wie Apache oder IIS veröffentlicht werden.

- **Unsignierte Updates erlauben** - wählen Sie diese Option, um Updates und Installationen von einem lokalen Server zu erlauben.
- **Proxy verwenden** - wählen Sie diese Option, falls Ihr Unternehmen einen Proxy-Server verwendet. Die folgenden Einstellungen müssen angegeben werden:
 - ☐ **Server IP** - Geben Sie die IP-Adresse des Proxy-Servers ein.
 - ☐ **Port** - Geben Sie den Port ein, über den BitDefender die Verbindung zum Proxy-Server herstellt.
 - ☐ **Benutzername** - Geben Sie einen für den Proxy-Server gültigen Benutzernamen ein.
 - ☐ **Passwort** - Geben Sie das Passwort für den zuvor angegebenen Benutzer ein.

Klicken Sie auf **Anwenden**, um die Änderungen zu speichern.

10.4. Update Benachrichtigungen

BitDefender kann so eingestellt werden, dass Sie über bestimmte Ereignisse während des Betriebs benachrichtigt werden. Um festzulegen über welche Update-Ereignisse BitDefender Sie informieren soll, klicken Sie auf **Update** im Baummenü und dann auf den Tab **Benachrichtigungen**.



Update Benachrichtigungen

Wählen Sie die Update-Ereignisse, über die Sie informiert werden möchten:

- **Update durchgeführt** - wenn ein Update durchgeführt wurde.
- **Kein Update verfügbar** - wenn kein Update zur Verfügung steht.
- **Update fehlgeschlagen** - wenn ein Fehler während eines Updates aufgetreten und dieses fehlgeschlagen ist.
- **Produkt-Update verfügbar** - Wenn ein Produkt-Update zur Verfügung steht.

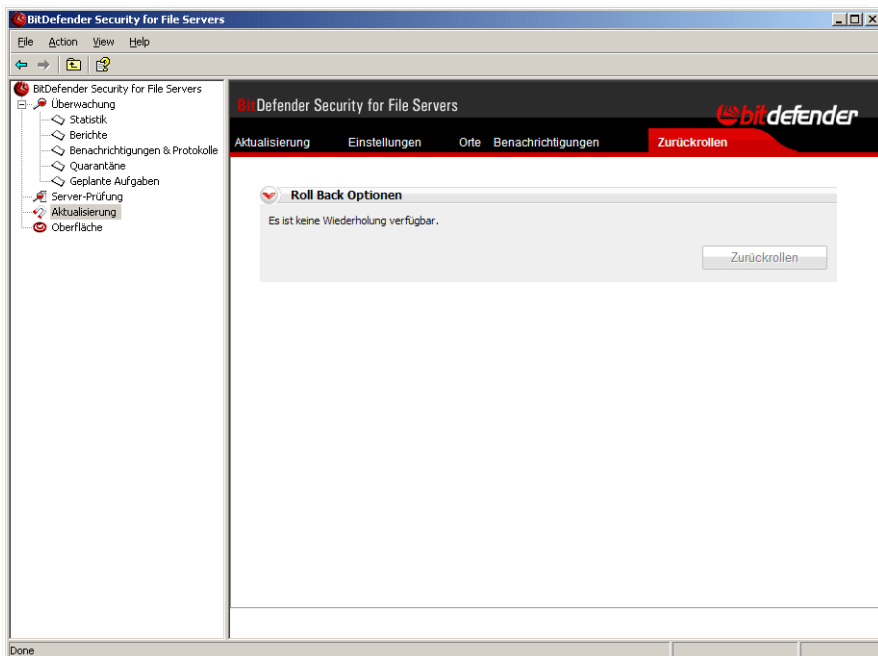
Um BitDefender so einzustellen, dass das Auftauchen eines Ereignisses protokolliert wird oder dass Sie darüber via Mail oder Net Send informiert werden, öffnen Sie **Benachrichtigungen & Protokolle** den Tab **Benachrichtigungen** und konfigurieren Sie das entsprechende Ereignis. Weitere Informationen finden Sie hier: [„Ereignisbenachrichtigung konfigurieren“ \(S. 53\)](#).

Klicken Sie auf **Anwenden**, um die Änderungen zu speichern.

10.5. Update zurückrollen

Wenn Sie seit der Erstinstallation von BitDefender ein Produkt Update durchgeführt haben, können Sie mit Hilfe der Rollback Funktion, zu der vorigen Produkt Version zurückkehren. Diese Funktion ist sehr nützlich, falls Ihr Produkt sich unerwartet verhält.

Um zu sehen, ob ein Rollback verfügbar ist, klicken Sie **Update** im Baummenu und dann **Rollback**.



Update zurückrollen

Wenn ein Rollback verfügbar ist, werden die aktuelle Produktversion und die Version, zu der Sie zurückrollen können, angezeigt. Klicken Sie **Roll Back** und bestätigen Sie Ihre Auswahl indem Sie im Bestätigungsfenster **Ja** klicken, um das Rollback auszuführen.

Wenn ein Rollback durchgeführt wurde, werden die aktuelle und die vorige Version angezeigt. Sie können den angegebenen Link benutzen, um zur neueren Version zurück zu Updaten.

11. Allgemein

Das allgemeine Snap-In bietet die Möglichkeit, BitDefender so zu konfigurieren, dass Berichte des BitDefender Labors bezüglich der auf dem Server gefundenen Viren und Vorfälle während des Produktbetriebs gesendet werden.

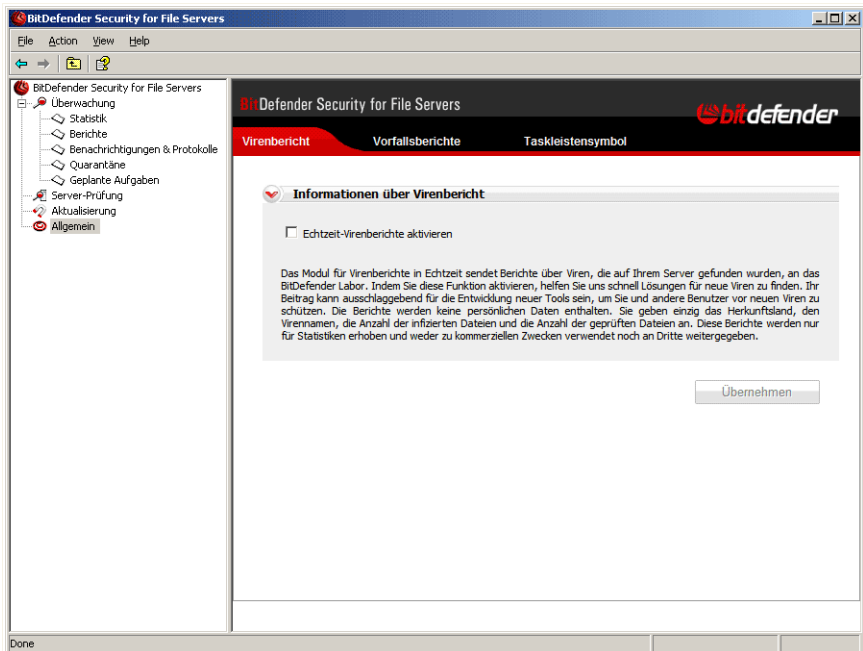
Hier können Sie auch allgemeine Einstellungen für das BitDefender-Taskleistensymbol vornehmen.

11.1. Virenbericht

Mit den Virenberichten in Echtzeit können Berichte über die gefundenen Viren auf Ihrem Server an das BitDefender Labor gesendet werden, um uns dabei zu helfen, neue Viren zu identifizieren und Lösungen für diese zu finden. Ihr Beitrag könnte grundlegend für die Entwicklung neuer Tools sein, um Sie und Andere vor Virenbedrohungen zu schützen.

Diese Berichte enthalten keine persönlichen Daten wie Name, IP-Adresse oder andere Angaben. Die bereitgestellte Information enthält den Namen des Landes, den Virennamen, die Anzahl der infizierten Dateien sowie die Gesamtzahl aller geprüften Dateien. Die eigentlichen Berichte werden ausschließlich für eine statistische Auswertung verwendet. Sie werden weder Drittparteien vorgelegt, noch in irgendeiner Form kommerziell verwendet.

Um Virenberichte in Echtzeit zu konfigurieren, klicken Sie auf **Allgemein** im Baummenu und dann auf den Tab **Virenbericht**.



Virenbericht

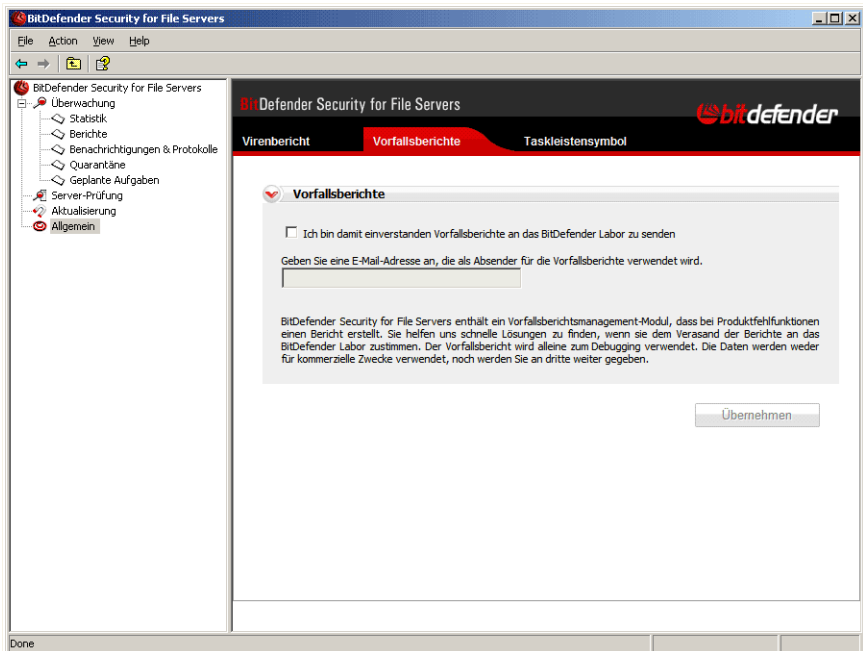
Virenberichte in Echtzeit sind standardmäßig deaktiviert. Um diese Funktion zu aktivieren, befolgen Sie folgende Schritte:

1. Wählen Sie **Virenberichte in Echtzeit aktivieren**.
2. Klicken Sie auf **Anwenden**, um die Änderungen zu speichern.

11.2. Vorfallsberichte

BitDefender Security for File Servers enthält ein Vorfall Management Modul, welches es erlaubt während eines Produktabsturzes Berichte zu erstellen. Durch Ihre Zustimmung Vorfallsberichte an das BitDefender Labor zu senden, helfen Sie uns schnelle Problemlösungen zu finden. Sie könnten einen großen Beitrag zur der Entwicklung eines stabilen Produktes machen, dass Ihren Wünschen entspricht. Die Berichte werden nur für statistische Zwecke genutzt, die Daten werden niemals kommerziell genutzt oder an dritte weitergegeben.

Um das Vorfalls Management Modul zu konfigurieren, klicken Sie **Allgemein** im Baummenu und dann **Berichte über Vorfälle**.



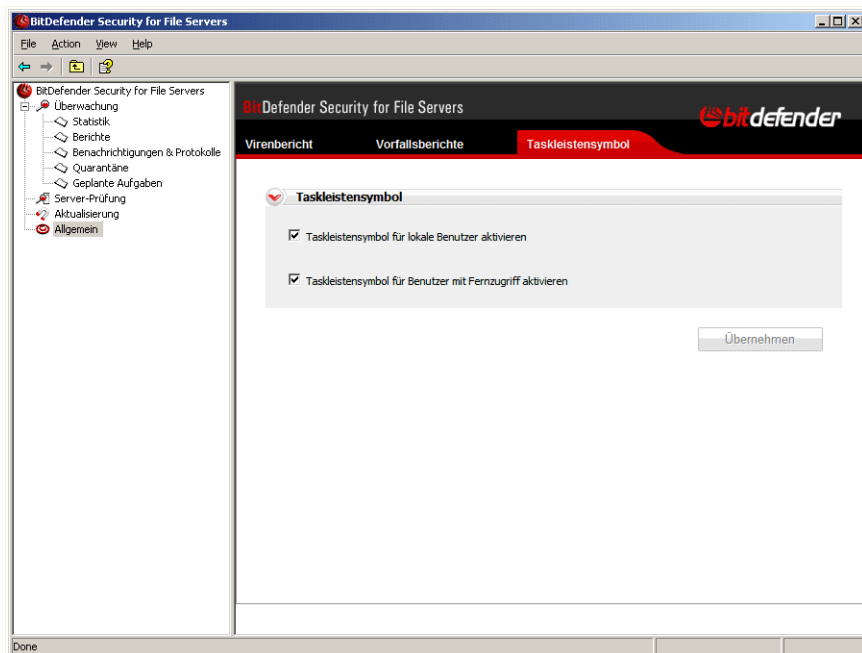
Vorfallsberichte

Standardmässig werden Berichte, die automatisch während eines Produktabsturzes erstellt wurden, nicht an das BitDefender Labor gesendet. Um BitDefender zu konfigurieren Vorfallsberichte an das BitDefender Labor zu senden, folgen Sie diesen Schritten:

1. Wählen Sie **Ich stimme zu, Berichte an das BitDefender Labor zu senden**.
2. Geben Sie Ihre E-Mail-Adresse an.
3. Klicken Sie auf **Anwenden**, um die Änderungen zu speichern.

11.3. Tray Icon

Um das Taskleistensymbol für verschiedene Benutzertypen zu aktivieren/deaktivieren, klicken Sie im Baummenü auf **Allgemein** und dann auf den Tab **Taskleistensymbol**.



Tray Icon

Sie können das Taskleistsymbol für lokale Benutzer oder über Remote Desktop verbundene Benutzer aktivieren/deaktivieren, indem Sie das entsprechende Kästchen markieren oder frei lassen.

Klicken Sie auf **Anwenden**, um die Änderungen zu speichern.



Beachten Sie

Die Änderungen werden angewendet, sobald der nächste Benutzer sich anmeldet.

Fehlerdiagnose und Problemlösung

12. BitDefender Konfigurationsreparatur Tool

Wenn Sie Störungen im BitDefender Security for File Server, nutzen Sie bitte das Bitdefender Konfigurationreparatur-Tool um die letzte bekannte gute Konfiguration wiederherzustellen. Das BitDefender Konfigurationsreparatur Tool speichert die Konfigurationsdatei jede Stunde, so dass Sie es wenn erforderlich wieder herstellen können. Dieses Tool kann erfolgreich verwendet werden, um ein korruptes Konfigurationsdateiproblem zu befestigen, das in äußersten Situationen wie eine erzwungene durch eine Gedächtnislücke verursachte Systemstilllegung vorkommen kann.

Um die letzte bekannte gute Version der Konfigurationsdatei wieder herzustellen, befolgen Sie diese Schritte:

1. Öffnen Sie das BitDefender-Konfigurationsreparatur-Tool auf folgende Weise:
Startmenü → Alle Programme → BitDefender Security for Windows Server → BitDefender-Konfigurationsreparatur-Tool.



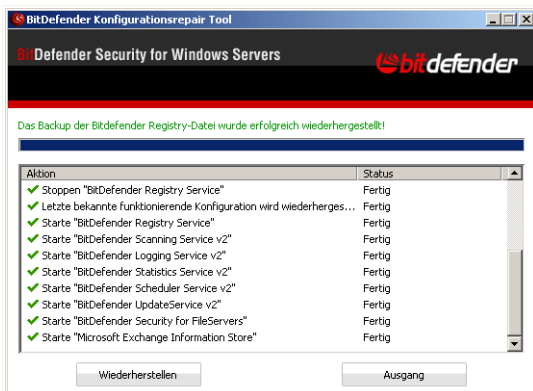
2. Klicken Sie auf **wiederherstellen**, um mit der Wiederherstellung der Sicherungskopie des Konfigurationsfile zu beginnen
3. Bitte warten bis Bitdefender KonfigurationsReparatur Tool die Wiederherstellungsprozess beendet.



Konfigurationsreparatur

Das Fenster zeigt den Status des Wiederherstellungsprozesses. Zuerst stoppt das BitDefender Konfigurationsreparatur Tool die Dienste von BitDefender Security for Servers Produkte, die auf dem System installiert sind (Dienste, die Anwendungen von Microsoft gehören, können auch angehalten werden; zum Beispiel, Microsoft Exchange Transport, wenn die BitDefender Security for Exchange installiert ist). Dann ersetzt das BitDefender Konfigurationsreparatur Tool die korrupte Konfigurationsdatei durch die Sicherungsdatei (eine ältere funktionierende Konfigurationsdatei). Schließlich startet das BitDefender Konfigurationsreparatur Tool wieder die vorher gestoppten Prozesse.

4. Das BitDefender Konfigurationsreparatur-Werkzeug informiert Sie, wenn die Sicherungskopie der Konfigurationsdatei erfolgreich wieder hergestellt worden ist.



Fertigstellen

Klicken Sie auf **Ausgang**, um dieses Fenster zu schließen.

13. Support

Als geschätzter Anbieter ist BitDefender stets bemüht, einen einmalig schnellen und sorgfältigen Support anzubieten. Sollten Probleme im Zusammenhang mit Ihrem BitDefender-Produkt auftreten oder Sie Fragen dazu haben, so wenden Sie sich bitte an unser **Online-Support-Center**. Dort gibt es verschiedene Ressourcen, mit deren Hilfe Sie schnell die richtige Lösung oder Antwort finden können. Sie können auch das Kundenbetreuungs-Team von BitDefender kontaktieren. Unsere Kundenbetreuer beantworten Ihre Fragen zügig und bieten Ihnen die benötigte Unterstützung.



Beachten Sie

Im Support-Center finden Sie weiterführende Informationen zu unseren Support-Leistungen und Support-Richtlinien.

13.1. BitDefender-Support-Center

Im BitDefender-Support-Center unter <http://www.bitdefender.de/businesshelp> unterstützen wir Sie in allen Belangen rund um Ihr BitDefender-Product.

Dabei stehen Ihnen verschiedene Ressourcen zur Verfügung, um die richtige Lösung oder Antwort zu finden:

- BitDefender Knowledge Base
- BitDefender Support-Forum
- Video Tutorials
- Produktdokumentation

Weitere Informationen über Computersicherheit, BitDefender-Produkte und unsere Firma finden Sie über Ihre Lieblingssuchmaschine.

13.1.1. BitDefender Knowledge Base

Bei der BitDefender Knowledge Base handelt es sich um eine Wissensdatenbank mit Informationen rund um Bitdefender Produkte. In leicht verständlicher Form bietet die Knowledge Base Informationen, Anleitungen und Berichte über neue Patches und behobene Probleme. Ebenfalls enthalten sind empfohlene Vorgehensweisen bei der Verwendung von Bitdefender Produkten und allgemeine Informationen wie z.B. Präventionsmaßnahmen vor Viren und anderen Schädlingen.

Die BitDefender Knowledge Base ist zudem öffentlich zugänglich und komplett durchsuchbar. Durch diese Art der Informationsbereitstellung bieten wir unseren Kunden eine weitere Möglichkeit, technische Grundlagen und Fachwissen über unsere Produkte zu erlangen.

Die BitDefender-Knowledge-Base für Unternehmensprodukte ist jederzeit unter <http://www.bitdefender.de/businesshelp> erreichbar.

13.1.2. BitDefender Support-Forum

Das BitDefender Support Forum bietet Anwendern eine Möglichkeit, Hilfe zu erhalten oder anderen Hilfestellung zu geben. Hier können Sie Ihre Probleme und Fragen rund um Ihr BitDefender-Produkt posten.

Support-Techniker von BitDefender überwachen neue Forumeinträge, um Ihnen helfen zu können. Außerdem können Sie eine Antwort auf Ihre Frage oder einen Lösungsvorschlag von einem bereits erfahrenen BitDefender-Anwender erhalten.

Bevor Sie einen Eintrag ins Forum stellen, suchen Sie bitte im Forum nach einem ähnlichen oder verwandten Themenbereich.

Das BitDefender Support Forum finden Sie unter <http://forum.bitdefender.com>. Es steht in fünf Sprachen zur Verfügung: Englisch, Deutsch, Französisch, Spanisch und Rumänisch. Mit einem Klick auf **Business Protection** gelangen Sie in den Bereich Unternehmensprodukte.

13.1.3. Video Tutorials

Die Video Tutorials leiten Sie Schritt für Schritt durch die Konfiguration des Produkts.

Ziel ist es, die Abhängigkeit von professioneller Unterstützung zu beenden und im Gegenzug die notwendigen Informationen zur Verwendung und Konfigurationen von BitDefender-Produkten in Video-Tutorials zur Verfügung zu stellen. So müssen Sie nicht erst beim BitDefender-Support anrufen, um Hilfe zu erhalten oder versuchen, komplizierte Verfahren umzusetzen. Sehen Sie sich ein Video-Tutorial an und folgen Sie den beschriebenen Schritten.

Die Video-Tutorials für die Unternehmensprodukte finden Sie unter **Support-Center** > Video-Tutorials.

13.1.4. Produktdokumentation

Die Produktdokumentation ist die umfassendste Informationsquelle rund um Ihr Produkt.

Unter **Support-Center** > Dokumentation stehen die neuesten Versionen der Dokumentationen für die BitDefender-Unternehmensprodukte zum Download bereit.

13.2. Hilfe anfordern

Nutzen Sie das Online-Support-Center, um Unterstützung anzufordern:

1. Rufen Sie <http://www.bitdefender.de/businesshelp> auf.
2. Durchsuchen Sie die Knowledge-Base nach Artikeln, die eine Lösung für Ihr Problem enthalten könnten.
3. Lesen Sie die relevanten Artikel oder Dokumente und probieren Sie die vorgeschlagenen Lösungen aus.

4. Sollten Sie keine entsprechende Lösung finden können, klicken Sie auf **Contact Us** im Menü auf der linken Seite.
5. Im Kontaktformular können Sie ein E-Mail-Support-Ticket eröffnen oder auf weitere Kontaktoptionen zugreifen.

Nähere Kontakt-Informationen finden Sie unter „*Kontaktinformation*“ (S. 157).

13.3. BitDefender Support Tool

Das BitDefender Support Tool erstellt ein ZIP-Archiv von Dateien, die von unseren Support-Technikern benötigt werden, um Probleme mit BitDefender Management Server zu untersuchen.

Um das Support Tool zu benutzen, folgen Sie diesen Schritten:

1. Öffnen Sie das BitDefender-Support-Tool über den folgenden Pfad: **Startmenü** → **Alle Programme** → **BitDefender Security for Windows Servers** → **BitDefender-Support-Tool**.



BitDefender Support Tool

2. Markieren Sie das Zustimmungskästchen und klicken Sie auf **Weiter**.

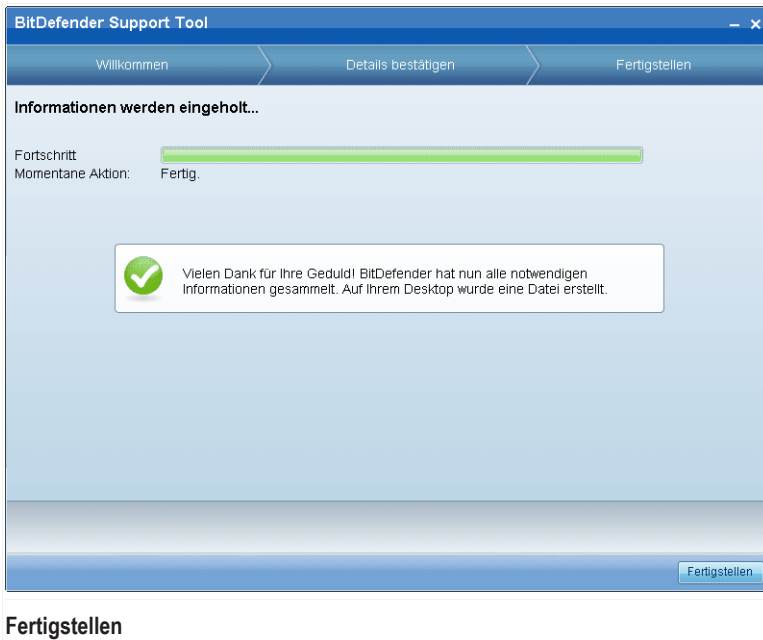
The screenshot shows the 'Übertragung der Details' (Transfer Details) window of the BitDefender Support Tool. The window has a blue header bar with the title 'BitDefender Support Tool' and standard window controls. Below the header is a navigation bar with three tabs: 'Willkommen', 'Details bestätigen', and 'Fertigstellen'. The 'Details bestätigen' tab is currently selected. The main area is titled 'Übertragung der Details' and contains a form with the following fields:

- E-Mail-Adresse*: A text input field.
- Vollständiger Name*: A text input field.
- Problemart*: A dropdown menu with 'Nicht spezifiziert' selected.
- Land*: A dropdown menu with 'Nicht spezifiziert' selected.
- Problembeschreibung*: A large text area for describing the problem.

Below the form, there is a note: '* Alle Felder sind Pflichtfelder.' (All fields are mandatory). At the bottom right of the window, there are two buttons: 'Weiter' (Next) and 'Abbrechen' (Cancel).

Übertragung der Details

3. Geben Sie in das Formular die nötigen Daten ein:
 - a. Geben Sie Ihre E-Mail-Adresse ein.
 - b. Geben Sie Ihren Namen ein.
 - c. Wählen Sie aus dem Menü die Art des Problems, das aufgetreten ist.
 - d. Wählen Sie Ihr Land aus dem entsprechenden Menü.
 - e. Beschreiben Sie im Textfeld das Problem, dass aufgetreten ist.
4. Klicken Sie auf **Weiter**. Das Support Tool sammelt Produktinformationen, Informationen zu anderen Anwendungen, die auf ihrem System installiert sind sowie die Software und Hardware Konfiguration.
5. Warten Sie, bis der Vorgang beendet ist.



Es wurde ein ZIP-Archiv auf Ihrem Desktop erstellt. Klicken Sie auf **Beenden**, um das Fenster zu schließen.

Sie können das .zip Archiv zusammen mit Ihrer Supportanfrage senden, um die Zeit zur Lösung Ihrer Anfrage zu reduzieren.

14. Kontaktinformation

Effiziente und kundenorientierte Kommunikation ist der Schlüssel zu einem erfolgreichen Geschäftsmodell. Seit mehr als 10 Jahren überbietet BITDEFENDER konstant die bereits hochgesteckten Erwartungen unserer Kunden und Partner und diese Tradition wollen wir auch in Zukunft fortführen. Für jedwede Fragen stehen wir Ihnen gerne zur Verfügung.

14.1. Kontaktadressen

Vertrieb: vertrieb@bitdefender.de
 Support-Center: <http://www.bitdefender.de/businesshelp>
 Dokumentation: documentation@bitdefender.com
 Lokale Vertriebspartner: <http://www.bitdefender.de/partners>
 Partner Programm: vertrieb@bitdefender.de
 Media Relations presse@bitdefender.de
 Jobs: jobs@bitdefender.de
 Virus Einsendungen: virus_submission@bitdefender.com
 Spam Einsendungen: spam_submission@bitdefender.com
 Report Abuse: abuse@bitdefender.com
 Webseite: <http://www.bitdefender.de>

14.2. Händler vor Ort

Die BitDefender Händler stehen für Fragen und Informationen in ihren jeweiligen Regionen jederzeit zur Verfügung, sowohl für vertriebliche als auch für allgemeine Anfragen.

So finden Sie einen BitDefender Distributor in Ihrem Land:

1. Rufen Sie <http://www.bitdefender.de/site/Partnership/list> auf.
2. Die Kontaktinformationen der lokalen BitDefender-Vertriebspartner sollten automatisch angezeigt werden. Sollte dies nicht der Fall sein, so wählen Sie Ihr Land aus, um die Informationen anzuzeigen.
3. Falls Sie in Ihrem Land keinen BitDefender Distributor finden, können Sie uns gerne unter vertrieb@bitdefender.de kontaktieren. Bitte schreiben Sie uns Ihre Email in englischer Sprache, damit wir Ihnen umgehend helfen können.

14.3. BitDefender Geschäftsstellen

Die BitDefender Niederlassungen stehen für Fragen und Informationen in ihren jeweiligen Regionen jederzeit zur Verfügung, sowohl für vertriebliche als auch für allgemeine Anfragen. Die genauen Kontaktdaten und Adressen finden Sie in der unten stehenden Auflistung.

14.3.1. Deutschland

BitDefender GmbH

Airport Office Center
Robert-Bosch-Straße 2
59439 Holzwickede
Deutschland

Telefon (Geschäftsstelle&Vertrieb): +49 (0)2301 91 84 222

Telefon (Technischer Support): +49 (0)2301 91 84 444

Vertrieb: vertrieb@bitdefender.de

Webseite: <http://www.bitdefender.de>

Support-Center: <http://www.bitdefender.de/businesshelp>

14.3.2. USA

BitDefender, LLC

PO Box 667588
Pompano Beach, FL 33066
United States

Telefon (Vertrieb&Technischer Support): 1-954-776-6262

Vertrieb: sales@bitdefender.com

Web: <http://www.bitdefender.com>

Support-Center: <http://www.bitdefender.com/businesshelp>

14.3.3. Großbritannien und Irland

Business Centre 10 Queen Street
Newcastle, Staffordshire
ST5 1ED
UK

Telefon (Vertrieb&Technischer Support): +44 (0) 8451-305096

E-Mail: info@bitdefender.co.uk

Vertrieb: sales@bitdefender.co.uk

Webseite: <http://www.bitdefender.co.uk>

Support-Center: <http://www.bitdefender.co.uk/businesshelp>

14.3.4. Spain

BitDefender España, S.L.U.

Avda. Diagonal, 357, 1º 1ª
08037 Barcelona
España

Fax: (+34) 93 217 91 28

Telefon (Geschäftsstelle&Vertrieb): (+34) 93 218 96 15

Telefon (Technischer Support): (+34) 93 502 69 10

Vertrieb: comercial@bitdefender.es

Webseite: <http://www.bitdefender.es>

Support-Center: <http://www.bitdefender.es/businesshelp>

14.3.5. Rumänien

BITDEFENDER SRL

West Gate Park, Building H2, 24 Preciziei Street

Bucharest, Sector 6

Fax: +40 21 2641799

Telefon (Vertrieb&Technischer Support): +40 21 2063470

Vertrieb: sales@bitdefender.ro

Webseite: <http://www.bitdefender.ro>

Support-Center: <http://www.bitdefender.ro/businesshelp>

Glossar

Adware

Adware ist häufig mit einer Absenderanwendung kombiniert, die kostenlos ist, solange der Nutzer die Adware akzeptiert. Adware Anwendungen müssen in der Regel installiert werden, nachdem der Nutzer einer Lizenzvereinbarung zugestimmt hat. In der Lizenzvereinbarung wird auch der Zweck der Anwendung genannt und somit liegt keine Rechtswidrigkeit vor.

Allerdings können Popup-Anzeigen mit der Zeit sehr lästig werden und in manchen Fällen die Systemperformance beeinträchtigen. Zudem kann aufgrund der Daten, die manche dieser Programme sammeln, die Privatsphäre von Nutzern verletzt werden, die sich über die Bedingungen in der Lizenzvereinbarung nicht völlig im Klaren waren.

AktiveX

AktiveX ist ein Programmuster, dass von anderen Programmen und Betriebssystemkomponenten unter Windows aufgerufen werden kann. Die ActiveX Technologie wird von Microsofts Internet Explorer benutzt, damit interaktive Webseiten eher wie Programme und nicht wie statische Seiten angezeigt werden. Mit ActiveX können die Benutzer z.B. Fragen stellen oder beantworten, Buttons verwenden, oder verschiedenartige Interaktionen mit der Webseite herstellen. ActiveX Controls werden oft in Visual Basic geschrieben.

Erwähnenswert ist, dass bei ActiveX die Sicherheitskontrollen fehlen, deshalb raten Computersicherheitsexperten davon ab, ActiveX über das Internet zu nutzen.

Aktualisierung

Neue Softwareversionen oder Hardwareprodukte, die eine ältere Version ersetzen. Die Update-Installationsroutine sucht nach älteren Versionen auf dem Rechner, da sonst kein Update installiert werden kann.

BitDefender hat sein eigenes Update Modul, welches das manuelle oder automatische Prüfen nach Updates ermöglicht.

Arbeitsspeicher

Interne Speicherzonen im Rechner. Der Begriff Arbeitsspeicher bedeutet Datenträger in Form von sehr schnellen Chips. Das Wort Speicher ist der Speicherplatz, der sich auf Magnetbändern oder Datenträgern befindet. Jeder Rechner hat eine gewisse Menge Arbeitsspeicher. Dieser wird auch Hauptspeicher oder RAM genannt.

Archive

Ein Datenträger, ein Magnetband oder ein Ordner mit Dateien, die von einer Datensicherung/BackUp erzeugt wurden.

Eine Datei, die eine oder mehrere Dateien in einem komprimierten Format enthält.

Backdoor (Hintertür)

Eine Sicherheitslücke eines Systems, die der Entwickler oder Verwalter absichtlich hinterlässt. Der Grund dafür muss nicht immer bösartig sein. Manche Betriebssysteme haben schon bei der Fabrikation privilegierte Konten, damit diese von den Kundendienst-Technikern oder Programmierern der Hersteller benutzt werden können.

Befehlszeile

Die Befehlszeile ist eine zeichenorientierte Benutzerschnittstelle. Die Kommunikation zwischen Benutzer und Computer findet ausschließlich durch die Eingabe von bestimmten Befehlen statt, die sich aus einzelnen Buchstabenfolgen zusammensetzen. Als Eingabegerät wird eine Tastatur benutzt. Die Verwendung einer Maus ist nicht möglich. Auf der Befehlszeile werden die einzelnen Anweisungen in einer bestimmten Befehlssprache eingegeben, die vom Computer und seiner Software ausgewertet und mit den entsprechenden Ergebnissen auf dem Ausgabegerät (meistens ein Monitor) wieder an den Benutzer übergeben werden.

Bootsektor

Der erste Sektor einer Festplatte oder Diskette. Hier liegen Daten, die das Betriebssystem zum Booten (Starten) braucht.

Bootvirus

Ein Virus, der den Bootsektor einer Festplatte oder eines Diskettenlaufwerks infiziert. Beim Versuch von einer Diskette, die mit einem Bootvirus infiziert ist, zu booten wird dieser im Arbeitsspeicher aktiviert. Bei jedem Neustart wird der Virus so im Arbeitsspeicher aktiviert und überträgt sich auf eingelegte Wechselmedien.

Cookie

In der Internetindustrie werden Cookies als kleine Dateien beschrieben, die Daten über einzelne Computer enthalten und die von den Werbern analysiert und verwendet werden, um die Interessen und Vorlieben der Benutzer herauszufinden. Die Cookie-Technologie wurde deshalb weiter entwickelt, damit der Benutzer nur solche Werbung zugeschickt bekommt, die seinen Interessen dient. Für viele ist es aber wie ein zweischneidiges Messer. Einerseits ist es wirksam und sachbezogen, da man nur Anzeigen, an denen man interessiert ist, betrachten kann, andererseits heißt es dem Benutzer "auf die Spur zu kommen" und ihn auf Schritt und "Klick" zu verfolgen. Es ist verständlich, dass der Datenschutz ein umstrittenes Thema ist und viele sich von dem Begriff als SKU-Nummern (die Streifencodes auf den Packungen, die im Geschäft an der Theke gescannt werden) betrachtet zu werden, angegriffen fühlen. Auch wenn dieser Gesichtspunkt extrem erscheint ist er manchmal korrekt.

Dateierweiterung

Der Teil hinter dem Punkt im Dateinamen. Die Erweiterung oder Extension beschreibt die Art der Daten, die in einer Datei gespeichert sind.

Viele Betriebssysteme benutzen Dateierweiterungen, z.B. Unix, VMS, MS-DOS. Sie enthalten gewöhnlich ein bis zwei Buchstaben (alte Betriebssysteme können nicht mehr als drei Buchstaben unterstützen), Beispiele dafür sind "c" für C-Quellcode, "ps" für PostScript oder "txt" für beliebige Texte. Windows zeigt bei ihm bekannten Dateitypen keine Dateierweiterung in der graphischen Benutzeroberfläche an, stattdessen wird häufig ein Symbol verwendet.

Download

Kopiert Daten (gewöhnlich eine ganze Datei) von einer Hauptquelle auf ein Peripheriegerät. Der Begriff bezeichnet oft den Kopiervorgang von einem Online Service auf den eigenen Rechner. Download oder Herunterladen kann auch das Kopieren einer Datei von einem Netzwerkserver auf einen Netzwerkrechner bedeuten.

Durchsuchen

Kurzform für Web-Browser, eine Softwareanwendung, die zum Lokalisieren und Anzeigen von Webseiten verwendet wird. Die bekanntesten Browser sind Netscape Navigator und Microsoft Internet Explorer. Beide sind graphische Browser, das heißt sie können sowohl Grafiken als auch Texte anzeigen. Weiterhin können die meisten Browser Multimedia-Informationen wie Klang- und Videodateien anzeigen, wobei sie für diverse Formate Plug-Ins (zusätzliche Softwarekomponenten) benutzen.

E-Mail

Elektronische Post. Ein Dienst, der Nachrichten an andere Rechner über ein lokales oder ein globales Netzwerk übermittelt.

E-Mail Client

Ein E-Mail Client ist eine Anwendung, die das Senden und Empfangen von E-Mails ermöglicht.

Ereignisanzeige

Ereignisse oder Erscheinungen, die in einem Programm vorkommen. Ereignisse können Benutzeraktionen, wie zum Beispiel Mausklicks oder Tastatureingaben, oder Systemereignisse, wie zum Beispiel ungenügender Speicher, sein.

Fehlalarm

Erscheint, wenn ein Virens Scanner eine Datei als infiziert erkennt, obwohl dies nicht der Fall ist. Kann bei heuristischem Virenprüfen auftreten.

Heuristik

Eine Methode, um neue Viren zu identifizieren. Diese Prüfmethode beruht nicht auf spezifische Virussignaturen. Der Vorteil einer heuristischen Prüfung ist, dass man nicht von einer neuen Virusvariante getäuscht werden kann. Manchmal kann auch ein verdächtiger Code in einem normalen Programm gemeldet werden, ein sogenannter Fehlalarm wird angezeigt.

IP

Internet Protocol - Das TCP/IP Protokoll ist verantwortlich für die korrekte IP Adressierung und die korrekte Zustellung der Datenpakete.

Java Applet

Ein Java Programm, das nur auf Webseiten läuft. Um ein Applet auf einer Webseite zu benutzen, gibt man den Namen und die Größe (Länge und Breite in Pixel) des Applets an. Wenn die Webseite abgerufen wird, lädt der Browser das Applet vom Server herunter und führt es auf der Benutzermaschine (dem Client) aus. Applets sind keine Anwendungen, da sie von strengen Sicherheitsprotokollen gesteuert werden.

Obwohl Applets auf dem Client laufen, können diese keine Daten auf der Clientmaschine lesen oder schreiben. Zusätzlich sind die Applets weiter begrenzt, so dass sie nur Daten aus der Domäne lesen und beschreiben können, die sie unterstützen.

Komprimierte Programme

Eine Datei in einem komprimierten Format. Viele Betriebssysteme und Anwendungen enthalten Befehle, die das Komprimieren einer Datei ermöglichen, so dass diese weniger Speicherplatz benötigt. Zum Beispiel: Angenommen Sie haben einen Text, der 10 aufeinander folgende Leerzeichen enthält. Normalerweise nehmen diese 10 Bytes Speicherplatz ein.

Ein Programm, das Dateien komprimiert, würde die Leerzeichen durch ein spezielles Zeichen „Leerzeichenreihe“ ersetzen, gefolgt von der Zahl der Leerzeichen, die ersetzt wurden. In diesem Fall sind nur noch zwei Bytes notwendig statt zehn. Das wäre ein Beispiel für eine Komprimierungstechnik, es gibt aber noch viele andere.

Laufwerk

Ein Gerät, das rotierende Speichermedien lesen und beschreiben kann.

Ein Festplatten-Laufwerk liest und beschreibt Festplatten.

Ein Disketten-Laufwerk liest und beschreibt Disketten.

Laufwerke können sowohl interner (im Rechner eingebaut) als auch externer (in einem Gehäuse, das an den Rechner angeschlossen wird) Art sein.

Logdatei (Berichtsdatei)

Eine Datei, die stattgefundenen Aktivitäten aufzeichnet. Zum Beispiel speichert BitDefender eine Logdatei mit den geprüften Pfaden, Ordnern und der Archivanzahl, aber auch die geprüften, infizierten oder verdächtigen Dateien.

Makrovirus

Eine Virusform, die in einem Dokument als eingebettetes Makro verschlüsselt wird. Viele Anwendungen, wie Microsoft Word und Excel, unterstützen mächtige Makrosprachen.

Diese Anwendungen ermöglichen das Einbetten eines Makros in ein Dokument, welches dann bei jedem Öffnen des Dokuments ausgeführt wird. Ein Makro ist eine Aufzeichnung des Ablaufs von Routineaufgaben innerhalb des makrofähigen Programms, das dann immer wieder verwendet werden kann.

Nicht heuristisch

Diese Prüfmethode beruht auf einer spezifischen Virussignatur. Der Vorteil einer nicht heuristischen Prüfung ist, dass diese nicht von einem Scheinvirus getäuscht werden kann, und dass dieser keinen falschen Alarm auslöst.

Pfad

Zeigt die Stelle an, an der sich eine Datei in einem Rechner befindet. Diese Pfadangaben enthalten gewöhnlich den hierarchischen Aufbau des Dateiverzeichnisses: Laufwerke, Ordner, Unterverzeichnisse, die Datei und ihre Erweiterung.

Der Weg zwischen zwei Punkten, wie zum Beispiel der Kommunikationskanal zwischen zwei Rechnern.

Phishing

Dabei wird eine E-Mail mit einer betrügerischen Absicht an einen Nutzer gesendet. Der Inhalt dieser E-Mail gibt vor, von einem bekannten und seriös arbeitenden Unternehmen zu stammen. Zweck dieser E-Mail ist es dann, private und geheime Nutzerdaten zu erhalten, worauf der Absender beabsichtigt, die Identität des Nutzers anzunehmen. Die E-Mail führt den Benutzer dann auf eine Webseite, in der er aufgefordert wird, vertrauliche Daten wie Kreditkartennummern, TAN's oder PIN's preiszugeben. Dies soll aus Gründen der Aktualisierung geschehen. Diese Webseiten sind jedoch gefälscht und wurden eigens für den Diebstahl dieser Daten eingerichtet.

Polymorpher Virus

Ein Virus, der seine Form mit jeder Datei, die er infiziert, ändert. Da diese Viren kein beständiges binäres Muster haben, sind sie sehr schwer zu erkennen.

Rootkit

Bei einem Rootkit handelt es sich um einen Satz von Softwarewerkzeugen, die einem Administrator Low-End Zugriff zu einem System verschaffen. Rootkits traten zunächst nur auf UNIX-Systemen auf und haben im Laufe der Zeit auch ihren Einzug auf Linux- und Windows-Systemen gehalten.

Die Hauptaufgabe eines Rootkits besteht darin, seine Existenz zu verstecken, indem Prozesse und Dateien versteckt werden, Anmeldedaten und Berichtsdateien zu fälschen und jegliche Art von Daten abzufangen.

Rootkits zählen von Haus aus nicht zu schadensverursachender Software, da Sie keine Schadroutinen besitzen. Jedoch verändern Sie die vom Betriebssystem zurückgegebenen Daten und verstecken auf diese Weise ihre Präsenz. Dennoch kann über ein solches Rootkit schädliche Software nachträglich eingeschleust werden, und auch der wirtschaftliche Schaden ist nicht zu unterschätzen.

Schnittstelle

Stelle eines Rechners, an die ein Gerät angeschlossen werden kann. Rechner haben verschiedenartige Schnittstellen. Intern gibt es Schnittstellen zum Anschluss von Festplatten, Grafikkarten und Tastaturen. Extern haben Rechner Schnittstellen zum Anschluss von Modems, Druckern und anderen Peripheriegeräten.

In TCP/IP und UDP Netzwerken, ein Endpunkt zu logischen Verbindungen. Die Schnittstellennummer gibt die Art der Schnittstelle an. Zum Beispiel, Schnittstelle 80 wird für HTTP Traffic verwendet.

Script

Ein anderer Begriff für Makro- oder Batchdatei. Ein Skript ist eine Befehlsliste, die ohne Benutzereingriff ausgeführt werden kann.

Spam

Junk-E-Mail oder Junk-Postings in Newsgroups. Im Allgemeinen versteht man darunter jede Art von unerwünschter E-Mail.

Spyware

Software, die unentdeckt vom Nutzer private und geheime Anwenderdaten überwacht und über seine Internetverbindung abrufen. Dies geschieht in der Regel zu Werbezwecken. Typischerweise werden Spyware-Anwendungen als verborgene Komponenten in Freeware- oder Sharewareprogrammen gebündelt, die aus dem Internet herunter geladen werden können. Es ist jedoch darauf hinzuweisen, dass die Mehrzahl der Shareware- und Freeware-Anwendungen frei von Spyware ist. Ist die Spyware einmal installiert, überwacht sie die Nutzeraktivitäten und überträgt diese Daten im Hintergrund an jemand anderen. Spyware kann auch Informationen über E-Mail-Adressen und sogar Kennwörter und Kreditkartennummern sammeln.

Einem Trojanischen Pferd ähnelt Spyware darin, dass die Anwender das Produkt unwissentlich gemeinsam mit etwas anderem installieren. Eine weit verbreitete Möglichkeit, ein Opfer von Spyware zu werden, ist der Download von bestimmten heute erhältlichen Peer-to-Peer-Dateiaustauschprogrammen (Direktverbindungen von Computern).

Abgesehen von den Fragen der Ethik und des Datenschutzes besteht Spyware den Anwender, indem sie Speicherressourcen seines Rechners nutzt und den Internetzugriff verlangsamt, indem über seine Internetverbindung Informationen an den Spyware-Heimatserver gesendet werden. Da Spyware Speicher und Systemressourcen verbraucht, können die im Hintergrund laufenden Anwendungen zu Systemabstürzen oder allgemeiner Systeminstabilität führen.

Startup Objekt (Autostart-Objekt)

Jede Datei, die sich in diesem Ordner befindet, öffnet sich, wenn der Rechner gestartet wird. Zum Beispiel ein Startbildschirm, eine Sounddatei, die abgespielt wird, wenn der Rechner gestartet wird, ein Erinnerungskalender oder Anwendungsprogramme können Autostart-Objekte sein. Gewöhnlich wird eine Alias-Datei (Verknüpfung) statt der eigentlichen Datei in diesen Ordner gelegt.

Symbolleiste

Die Symbolleiste wurde mit Windows 95 eingeführt und befindet sich auf der Windows Taskleiste (gewöhnlich unten rechts, dort wo sich auch die Uhrzeit befindet). Er enthält kleine Icons zur Information und zum leichteren Zugriff, zum Beispiel: Fax, Drucker, Modem, Lautstärke und mehr. Um auf die Details und Steuerungen zuzugreifen, ist ein Doppelklick oder ein Klick mit der rechten Maustaste erforderlich.

TCP/IP

Transmission Control Protocol/Internet Protocol - Im Internet werden eine Vielzahl von verschiedener Hardware und Betriebssystemen miteinander verbunden. TCP/IP bietet eine Möglichkeit, all diese unterschiedlichen Komponenten zu Kommunikationszwecken miteinander zu verbinden.

Trojaner

Ein vernichtendes Programm, das sich als eine freundliche Anwendung tarnt und auftritt. Im Unterschied zu Viren vervielfältigen sich die Trojaner (auch "trojanische Pferde" genannt) nicht, aber sie können zerstörerisch sein. Einer der heimtückischsten Trojaner ist ein Programm, das behauptet Ihren Rechner von Viren zu befreien, stattdessen aber den Rechner infiziert. Viele Trojaner öffnen den Rechner für den Zugriff von außen.

Der Begriff entstammt einer Geschichte in Homer's "Ilias", in der die Griechen Ihren Feinden, den Trojanern, angeblich als Sühnegabe ein hölzernes Pferd schenkten. Aber, nachdem die Trojaner das Pferd innerhalb der Stadtmauern gebracht hatten, kamen die in dem Bauch des hölzernen Pferdes versteckten Soldaten heraus, öffneten die Tore der Stadt und ermöglichten somit ihren Landsmännern in die Stadt einzudringen und auf diese Weise Troja zu besetzen.

Virus

Ein Programm oder ein Codestück, das auf einen Rechner geladen wird, ohne dass der Benutzer Kenntnis davon hat und welches sich allein ausführt. Die Resultate von Viren können einfache Scherzmeldungen aber auch die Zerstörung von Hardware sein. Die meisten Viren können sich selber vervielfältigen. Alle Computerviren sind von Menschenhand geschrieben. Ein Virus, der sich immer wieder vervielfältigen kann ist sehr einfach zu schreiben. Sogar ein solch einfacher Virus ist fähig, sich durch Netzwerke zu verschicken und Sicherheitssysteme zu überbrücken.

Virusdefinition

Ein binäres Virusmuster, das von einem AntiVirus Programm verwendet wird, um einen Virus zu entdecken und zu entfernen.

Wurm

Ein Programm, das sich über ein Netzwerk verbreitet. Es kann sich nicht an andere Programme anhängen.